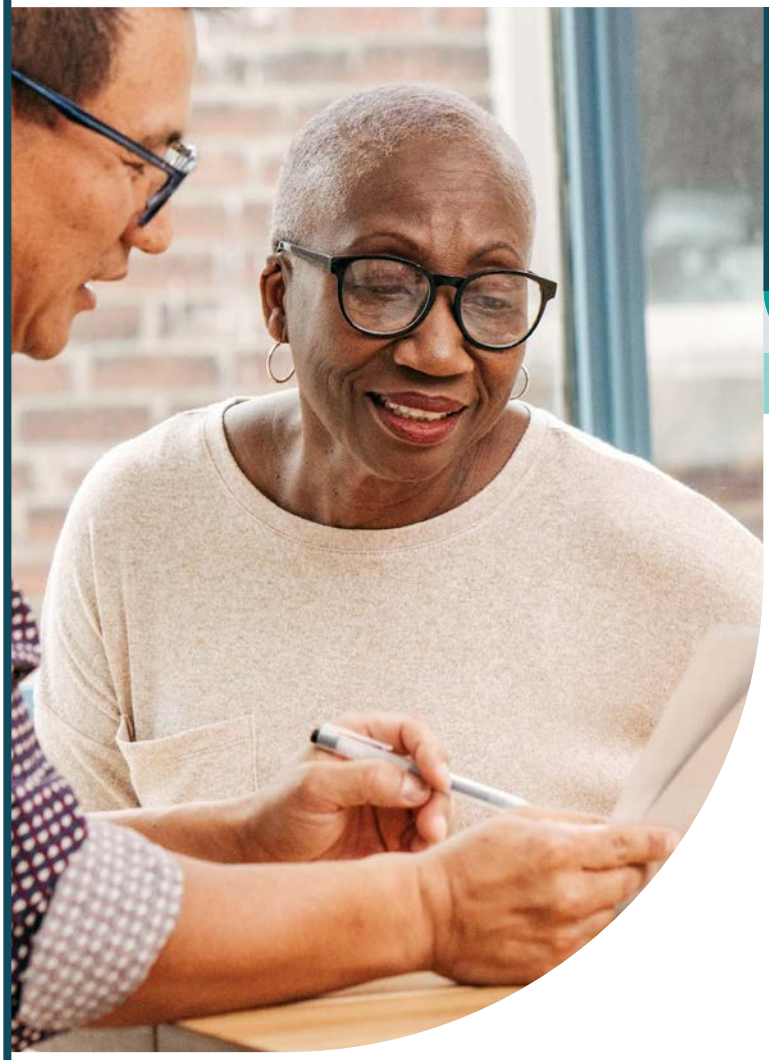
MANUAL PARA PARTICIPANTES

Savvy Saving Seniors®



Pasos para evitar estafas

BANK OF AMERICA

nco national council on aging®

CONTENIDO

¿Cuánto sabes? 3

Cuestionario: ¿Cuánto sabes sobre las estafas? 3

Respuestas del cuestionario 5

La docena sucia: Las 12 principales estafas dirigidas a adultos mayores 7

Caso de estudio: Una mirada más cercana a las estafas más comunes 22

Consejos para evitar estafas 23

Protégete a ti mismo y a los demás 29

Denunciar estafas y otros pasos para víctimas de fraude financiero 29

Recursos útiles 30

Apéndice A 31

Fiscales generales: Estados 31

Fuentes 33

Notas 34

¿Cuánto sabes?

CUESTIONARIO: ¿Cuánto sabes sobre las estafas?

1. **¿Qué hace que los delitos financieros contra los adultos mayores sean tan devastadores?**
   a. Perder una gran suma durante la jubilación es difícil o imposible de recuperar.
   b. Muchos adultos mayores ya viven con ingresos fijos o limitados.
   c. Las víctimas pueden no darse cuenta de que han sido estafadas debido al uso de herramientas de inteligencia artificial (IA).
   d. Todo lo anterior

2. **¿Puedes estimar cuánto dinero total perdieron los estadounidenses mayores en 2023 debido a estafas financieras?**
   a. 5.2 millones de dólares
   b. 650 millones de dólares
   c. 3,400 millones de dólares

3. **¿Qué situación financiera hace que un adulto mayor sea un blanco fácil para las estafas financieras?**
   a. Tener ingresos altos o un patrimonio sustancial
   b. Tener bajos ingresos y pocos ahorros
   d. Todo lo anterior

4. **Es seguro confirmar o proporcionar tu información de identificación personal, como tu número de Seguro Social, por teléfono siempre que tu identificador de llamadas muestre que es la Administración del Seguro Social quien llama.**
   a. Verdadero
   b. Falso

5. ¿Qué tipos de estafas utilizan tecnología de IA?

a. Estafas románticas

b. Estafas de soporte técnico

c. Estafas de inversión

d. Todo lo anterior

6. El término "phishing" (suplantación de identidad) se refiere a:

a. Realizar una búsqueda en Internet

b. La transferencia de criptomonedas de la víctima al estafador

c. La manera en que la generación Z escribe "fishing"

d. Métodos utilizados para engañarte y lograr que compartas información de identificación personal o de tu cuenta

7. Obtuviste una excelente cotización para algunas reparaciones muy necesarias en el hogar. El contratista tuvo la amabilidad de compartir que se espera que los precios de los materiales se disparen cualquier día. Pagar el total por adelantado es la mejor opción porque el contratista dice que es la única manera de fijar el precio.

a. Verdadero

b. Falso

8. Los sospechosos habituales que podrían querer estafarte incluyen:

a. Extraños

b. Familiares

c. Cuidadores

d. Todo lo anterior

Respuestas del cuestionario:

1. **D.** Todo lo anterior. Los delitos financieros contra los adultos mayores pueden ser devastadores y a menudo dejan a las víctimas sin forma de recuperar sus pérdidas. Esto puede ser especialmente perjudicial si el adulto mayor ya vive con un ingreso fijo o limitado. Las herramientas de IA han agregado un nivel de sofisticación a las tácticas de estafa, y es posible que ni siquiera te des cuenta de que has sido estafado, lo que potencialmente permite que la estafa continúe.

2. **C.** Según la Oficina Federal de Investigaciones (FBI), en 2023, más de 101,000 adultos de 60 años o más denunciaron haber sido víctimas de fraudes y estafas financieros. ¿El daño? Más de 3,400 millones de dólares en pérdidas, un aumento de aproximadamente el 11 % respecto al año anterior.[1] La pérdida monetaria promedio para una víctima de fraude a una persona mayor en 2023 ascendió a $33,915.

3. **C.** Todo lo anterior. Las estafas están dirigidas a personas de todos los niveles de ingresos. Los adultos mayores controlan una cantidad sustancial de la riqueza personal. Los estafadores, como los familiares y los cuidadores, son conscientes de la riqueza y de las vulnerabilidades de aquellos que la tienen. Las personas con ingresos más bajos a menudo son el objetivo porque pueden estar más dispuestas a correr un riesgo si algo suena demasiado bueno para ser verdad.

4. **B.** Falso. Utilizando tecnología especial, los estafadores pueden falsificar el número de teléfono real de una agencia gubernamental o llaman desde el mismo código de área (202 para Washington D. C., por ejemplo). Ver el número de teléfono real de la agencia gubernamental o el nombre en el identificador de llamadas puede engañarte y hacerte creer que la persona que llama es quien dice ser. Como regla general, las agencias gubernamentales como la Administración del Seguro Social, el Servicio de Impuestos Internos y Medicare nunca te llamarán ni te contactarán en línea para solicitarte información de identificación personal.

5. **D.** Todo lo anterior. La IA no se limita a los delitos informáticos o tecnológicos. El uso de la IA ha acelerado enormemente la escala, la velocidad y la sofisticación de todos los tipos de estafas financieras, haciendo que sea más difícil detectarlas y defenderse de ellas. La minería de datos para identificar mejor a las víctimas potenciales, el contenido generado por IA para falsificar credibilidad, la clonación de voz y los videos ultrafalsos para engañar al espectador: estas son solo algunas de las herramientas de IA que emplean los estafadores hoy en día.

6. **D.** La suplantación de identidad es un tipo de ataque que utiliza diversos métodos para intentar obtener tu información de identificación confidencial, información de cuentas financieras y contraseñas. Los correos electrónicos, los mensajes de texto y las llamadas telefónicas parecen provenir de una fuente legítima; y muchas veces te solicitarán que hagas clic en un enlace o que confirmes o proporciones la información que buscan. Las tecnologías de IA han hecho que la suplantación de identidad sea más efectiva, eludiendo los filtros de correo no deseado y engañando a muchos.

7. **B.** Falso. Esto suena como la clásica versión de reparación de viviendas de una estafa de confianza, en la que el delincuente primero se gana la confianza de su objetivo, le hace una oferta que es demasiado buena para ser verdad y luego no entrega el servicio o los bienes. Nunca pases a la siguiente etapa con un contratista sin un contrato firmado y nunca pagues el total por adelantado. Espera hasta que el trabajo esté completo y pase la inspección.

8. **D.** Todo lo anterior. Si bien muchos estafadores son desconocidos o miembros de una organización criminal más grande, las personas que tú conoces también pueden ser abusadores financieros. Esto no significa que debas aislarte, pero sí que debes permanecer alerta a las motivaciones y las acciones de quienes te rodean. Revisa tus cuentas y limita el acceso de otras personas a ellas.

Fraude:

Un término legal amplio que abarca actividades deshonestas destinadas a obtener beneficios financieros o personales.

Estafa:

Un tipo de fraude que implica engañar a alguien para que proporcione dinero o información personal.

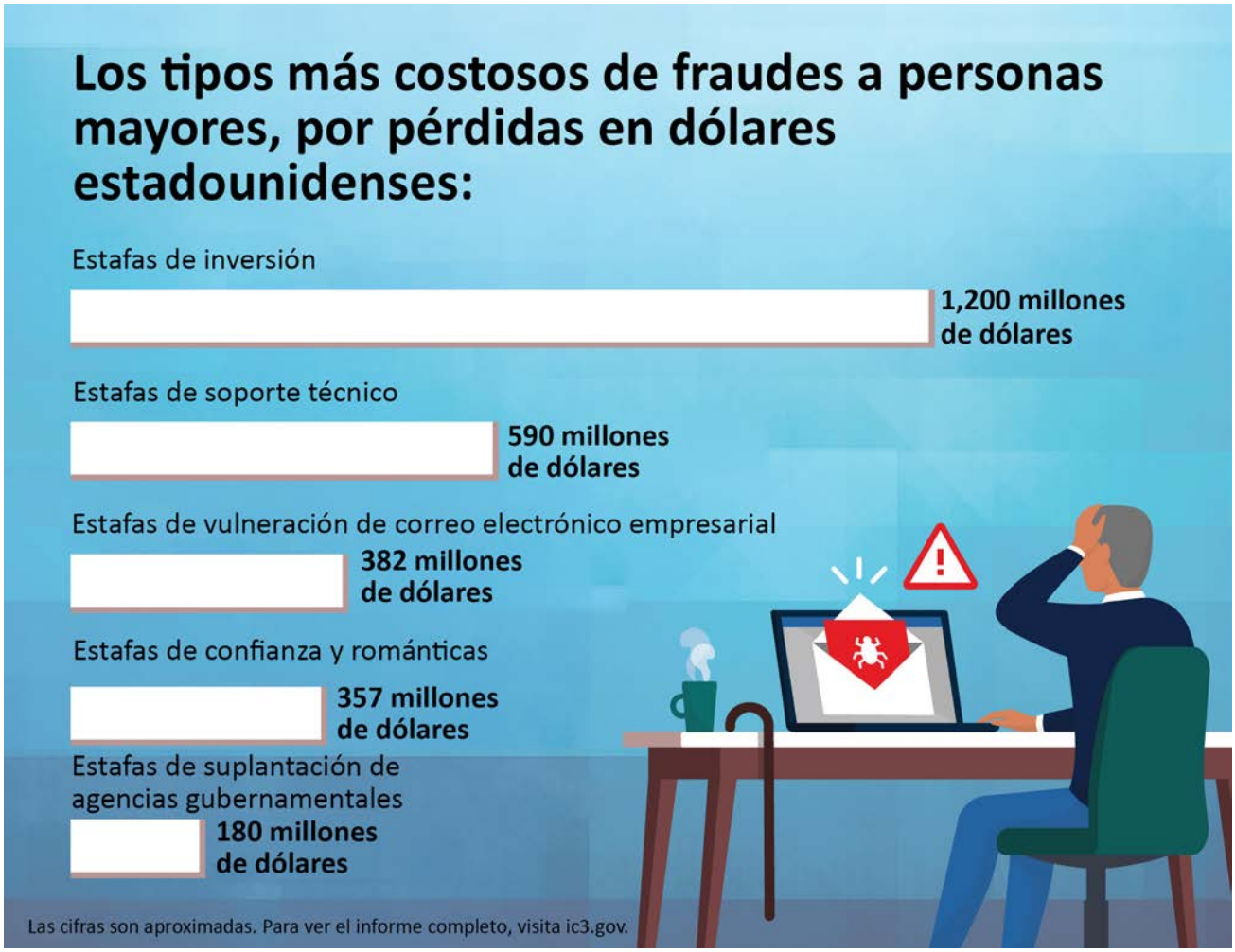
La docena sucia: Las 12 principales estafas dirigidas a adultos mayores

Cada día, el Centro de Denuncias de Delitos en Internet del FBI, también conocido como "IC3", registra miles de denuncias sobre una amplia variedad de estafas, muchas de ellas dirigidas a adultos mayores.

Si bien las estafas de centros de llamadas y de soporte técnico fueron el tipo de fraude a personas mayores más denunciado en 2023, con casi 18,000 denuncias ante el IC3, las estafas de inversión fueron las más costosas. Este tipo de delito financiero por sí solo les costó a las víctimas mayores más de 1,200 millones de dólares en pérdidas en 2023.[1] Aquí aprenderemos a reconocer este tipo de estafa, junto con el resto de la docena sucia: las 12 estafas más denunciadas dirigidas a adultos mayores.

También centraremos la atención en la IA para arrojar luz sobre cómo la rápida evolución de las tecnologías está contribuyendo potenciar estas estafas.

Fuente: Centro de Denuncias de Delitos en Internet del FBI, https://www.fbi.gov/news/stories/elder-fraud-in-focus



Fuente: Centro de Denuncias de Delitos en Internet del FBI, https://www.fbi.gov/news/stories/elder-fraud-in-focus

1. Estafas de centros de llamadas y de soporte técnico

Los centros de llamadas ilegales defraudan a miles de personas cada año y se dirigen deliberadamente a los adultos mayores. De hecho, las personas de 60 años o más perdieron más dinero en estas estafas que todos los demás grupos de edad juntos y afirman haber tenido que rehipotecar sus hogares o ejecutar una hipoteca, vaciar sus cuentas de jubilación, y pedir dinero prestado a familiares y amigos como resultado. Esta estafa funciona de distintas maneras.

En muchas estafas de soporte técnico, la persona que llama se hace pasar por un representante de soporte técnico, a menudo de una empresa conocida, y ofrece solucionar un problema informático inexistente. En otras ocasiones, pueden ofrecerle programas de protección antivirus. Para hacer cualquiera de estas dos cosas, el estafador a menudo te pide la contraseña de tu computadora y obtiene acceso remoto. Una vez dentro, pueden instalar programas maliciosos que les proporcionan acceso a largo plazo a la información personal y financiera en tu computadora.

Estafas de soporte técnico similares vienen en forma de correos electrónicos o ventanas emergentes que simulan un software antivirus. Estas estafas engañan a las víctimas para que hagan clic en un enlace y descarguen un programa antivirus falso o un virus real que permitirá al estafador acceder a la información del usuario en la computadora.

Una forma más nueva es la estafa del "jáquer fantasma". Comienza con la estafa de soporte técnico, pero también agrega impostores de una institución financiera y de una agencia gubernamental para agregar legitimidad a sus afirmaciones y convencerte de seguir sus instrucciones. La estafa del jáquer fantasma tiene tres fases:

1. **Fase 1:** Después de que el estafador de soporte técnico tenga acceso a tu computadora, afirmará que tus cuentas están en riesgo y te pedirá que inicies sesión en tus cuentas financieras, lo que le permite identificar tus cuentas más lucrativas para la segunda fase. La persona de soporte técnico te informa que un funcionario bancario se comunicará contigo para proteger tus cuentas en riesgo.
2. **Fase 2:** Un segundo estafador llama haciéndose pasar por tu institución financiera y describe una amenaza sobre tus cuentas, como un jáquer extranjero. Afirmará que la única forma de proteger tu dinero es transferirlo a una cuenta "segura" en la Reserva Federal o en otra agencia gubernamental. Los estafadores a menudo te piden que transfieras tu dinero mediante transferencia bancaria, efectivo o criptomonedas.
3. **Fase 3:** El tercer estafador dice ser de la Reserva Federal o de una agencia gubernamental, actuando como máxima autoridad para lograr que sigas las instrucciones. Si expresas dudas, el estafador te proporcionará documentos "oficiales" falsos en papel membretado de apariencia auténtica para respaldar su afirmación.

Enfoque en la IA: Las estafas de soporte técnico existen desde hace mucho tiempo, pero recientemente han recibido un gran impulso gracias a la tecnología de la inteligencia artificial. Con la IA, los estafadores pueden crear correos electrónicos que parezcan completamente auténticos, que eludan los filtros de correo no deseado y que contengan información personalizada recopilada sobre ti a partir de varias fuentes en línea. Esto es lo complicado de las estafas respaldadas por la IA. Añade un nivel de sofisticación al ataque, lo que ayuda a enmascarar las señales de alerta.

2. Estafas de violación de datos personales

Las estafas de violación de datos personales utilizan tácticas similares a las de los centros de llamadas y de soporte técnico, pero se diferencian en que son un delito de oportunidad. Aprovechando casos de violaciones de datos reales, los delincuentes explotan las preocupaciones reales de las personas enviándoles correos electrónicos o mensajes de texto que parecen alertas legítimas.

Estos mensajes, que advierten que tu información personal se vio comprometida en una violación de datos, a menudo motivan una acción inmediata para proteger tus cuentas. En realidad, estos estafadores utilizan enlaces o sitios web falsos para robar tu información personal confidencial o para instalar programas maliciosos en tus dispositivos.

Si fuiste parte de la violación de datos original y se filtró tu número de teléfono, el estafador puede llamarte directamente haciendo suplantación de identidad para obtener información personal adicional o para obtener acceso a tu computadora.

Enfoque en la IA: La IA generativa ayuda a estos oportunistas creando mensajes que pueden pasar desapercibidos a través de tus primeras líneas de defensa, como los filtros de correo electrónico no deseado. La IA también ayuda a estos estafadores a superar la última línea de defensa: ¡tú! Los algoritmos de la IA pueden localizar y analizar enormes cantidades de datos sobre innumerables objetivos para producir mensajes de suplantación de identidad altamente personalizados y de apariencia legítima. Si fuiste parte de la violación de datos inicial, la IA también puede incorporar los datos robados para hacer que estos mensajes sean aún más convincentes.

3. Estafas de confianza

Las estafas de confianza pueden ser particularmente dolorosas debido a la capa adicional de traición a nivel personal. Este tipo de delito financiero generalmente ocurre cuando un estafador defrauda a una persona después de haber ganado su confianza, a menudo utilizando la manipulación emocional y la explotación. Esto también puede ocurrir cuando el delincuente se hace pasar por alguien que le importa al adulto mayor, y la IA ha hecho que esto sea aún más factible. Veamos algunos ejemplos de este tipo de estafa:

- **Estafas románticas:** Los estafadores que crean personajes ficticios en sitios de citas y en redes sociales para atraer a adultos mayores a tener relaciones románticas no demuestran ningún respeto. Los delincuentes suelen “bombardear” con amor a sus objetivos para ganarse su afecto y su confianza rápidamente. Luego, crean escenarios en los que necesitan dinero de sus víctimas o cubrir los gastos de viaje para visitarlas. Los estafadores también pueden pedirles a los adultos mayores que depositen cheques o envíen paquetes por ellos. Sin embargo, es posible que la víctima esté participando sin saberlo en una actividad ilegal.

Las estafas románticas también pueden evolucionar a casos de sextorsión si el estafador llega a poseer fotografías íntimas. En 2023, personas de 60 años o más denunciaron 3,318 denuncias de sextorsión con pérdidas que superaron los 6 millones de dólares.

- **Estafa a los abuelos:** La estafa a los abuelos es muy exitosa porque utiliza uno de los activos más confiables de los adultos mayores: sus corazones. Los delincuentes llaman haciéndose pasar por un ser querido más joven (como un nieto, una sobrina o un sobrino) y dicen que están en problemas. Crean un sentido de urgencia necesario para rescatarlos de la situación, solicitando dinero de inmediato. Una señal reveladora de que tal situación es una estafa es que la persona en problemas te pedirá que envíes el dinero a través de Western Union o MoneyGram, a través de un amigo, o mediante algún otro método de pago extraño.
- **Estafas de contratistas o por reparaciones de vivienda:** Toc, toc. ¿Quién es? Un estafador. Los estafadores conducen por los vecindarios en busca de viviendas que puedan necesitar reparaciones y que estén ocupadas por adultos mayores. Una vez que la víctima fue identificada, el estafador le ofrece un presupuesto asequible para el trabajo propuesto, un trabajo que no tiene intención de hacer bien o en absoluto. Después de que la víctima paga el trabajo en efectivo o con cheque, el delincuente realiza reparaciones descuidadas, comienza pero no termina las reparaciones o desaparece por completo. Estos individuos son muy difíciles de localizar posteriormente, dejando al adulto mayor sin dinero y a veces con una casa en peores condiciones que antes.
- **Estafas que aprovechan la muerte o el funeral del cónyuge:** Lamentablemente, muchos estafadores ven la tragedia como una oportunidad y se aprovechan de los adultos mayores en sus momentos más vulnerables. Algunos estafadores leen obituarios y luego realizan llamadas o asisten al funeral para aprovecharse de la viuda o del viudo. El estafador alega que la persona fallecida tenía una deuda pendiente que debe pagar. Otras veces, las funerarias sin escrúpulos agregan cargos innecesarios o utilizan tácticas de venta agresivas a fin de presionar para que se contraten servicios más caros de lo necesario.

Enfoque en la IA: La IA se ha convertido en la herramienta preferida para muchas estafas de confianza debido a su capacidad de crear imitaciones hiperrealistas, videos manipulados y audios con voz clonada. Solo se necesitan unos pocos segundos de audio para que la IA clone la voz de una persona, que luego los estafadores usan para llamar a adultos mayores mientras se hacen pasar por familiares, amigos o incluso celebridades y figuras públicas en llamadas telefónicas o en mensajes de video.

La IA también puede generar videos realistas de personas haciendo o diciendo prácticamente cualquier cosa que el estafador pueda imaginar. Estos videos, llamados "ultrafalsos", se utilizan para engañar a personas, quienes pueden creer que están en una nueva relación romántica, se han hecho amigos de una celebridad o necesitan ayudar a un ser querido. Fotografías, guiones, sitios web, materiales comerciales y otros elementos convincentes se utilizan mucho más fácilmente en estafas de confianza con el uso de tecnologías de la IA.

4. Estafas por falta de pago o por falta entrega

En pocas palabras, las estafas por falta de pago o por falta de entrega ocurren cuando una transacción termina siendo unilateral. Por ejemplo, se proporciona un bien o un servicio, pero nunca se paga, o se paga un bien o un servicio, pero nunca se recibe. Las estafas de cebo y cambio, en las que un vendedor seduce al comprador con una oferta o producto atractivo, pero luego lo cambia por un producto diferente o inferior cuando lo entrega, también entran en esta categoría.

En las estafas por falta de pago, los delincuentes primero se aseguran de que les entregues el bien y luego nunca te lo pagan. Es posible que inicialmente proporcionen un pago que resulte ser una tarjeta de crédito robada o un cheque falso, retrasen continuamente el pago con una serie de excusas, o desaparezcan por completo. Solicitar métodos o condiciones de pago inusuales, o no recibir comunicación por parte del comprador son señales de alerta de este tipo de estafa.

Las características de las estafas por falta de entrega incluyen ofertas que parecen demasiado buenas para ser verdad, listados de productos que desaparecen después de la compra, presión para comprar rápidamente, métodos de pago inusuales y un comprador que se queda sin producto o sin reembolso.

Enfoque en la IA: Los estafadores pueden usar la IA para crear fácilmente tiendas en línea falsas y llenarlas con listados de productos falsos. A menudo, publican productos populares que son difíciles de encontrar en otro lugar o productos caros que tienen descuentos a precios increíblemente bajos. De cualquier manera, los productos no existen o serán reemplazados por sustitutos deficientes sin tu consentimiento.

5. Estafas de inversión

Desde esquemas Ponzi como el que se hizo famoso por Bernie Madoff (que defraudó a miles de personas, incluidas celebridades, por miles de millones de dólares) hasta correos electrónicos de un legendario príncipe nigeriano que busca un socio para reclamar el dinero de su herencia, hasta complejos productos financieros que ni siquiera muchos economistas entienden, los esquemas de inversión han sido durante mucho tiempo un método exitoso para aprovecharse de los adultos mayores. Este tipo de estafa a menudo se manifiesta en esquemas de pago por adelantado, esquemas Ponzi, esquemas piramidales, fraudes de manipulación del mercado, inversiones inmobiliarias e inversiones basadas en la confianza, como estafas de inversión en criptomonedas.

¿Crees que no te podría pasar a ti? Piénsalo otra vez. Curiosamente, estas estafas suelen comenzar con una estafa de confianza. El delincuente sabe que debe ganarse tu confianza para que inviertas grandes sumas de tu dinero duramente ganado en él, y lo hace a través de la amistad, el romance y la red profesional. En 2023, el IC3 del FBI recibió más de 6,400 denuncias de estafas de inversión de personas de 60 años o más con pérdidas declaradas de más de 1,200 millones de dólares.[1]

Los estafadores de inversiones, descritos como conocedores de la ingeniería social que se aprovechan de la confianza, pueden trabajar solos o en compañía de otros. Incluso podría tratarse de una persona nueva que conociste a través del estafador y que desempeña el papel de una de las historias de éxito del inversor. Es posible que te revelen el secreto o que, accidentalmente, deslicen información sobre su éxito delante de ti. A veces, pueden hacer alarde de lo que parece ser una riqueza extravagante, incitándote a que finalmente les preguntes cómo hacen para que les vaya tan bien. Por supuesto que todos son métodos calculados para introducir su esquema de inversión.

¿Y cómo podemos reconocer estos esquemas antes de que sea demasiado tarde? ¿Es la inversión compleja y difícil de entender? ¿Se presenta como si implicara poco o ningún riesgo? ¿Se presenta como si tuviera recompensas garantizadas o excepcionalmente altas? ¿Te lo sugirió alguien relativamente nuevo en tu vida? Una buena regla general para seguir: si suena demasiado bueno para ser verdad, ¡probablemente no sea cierto!

Enfoque en la IA: El fraude de inversiones se ve particularmente potenciado por las tecnologías de la IA tanto generativa como predictiva. Los estafadores utilizan videos ultrafalsos, clonación de voz y contenido generado por la IA para engañar a los inversores. Identidades falsas, empresas inexistentes y recomendaciones convincentes (como videos ultrafalsos que muestran a una celebridad o figura confiable recomendando una oportunidad de inversión) son todas herramientas del oficio. El Departamento de Seguros, Valores y Banca del Distrito de Columbia señala que con regularidad encuentra delincuentes que se hacen pasar por personal de la Comisión de Bolsa y Valores de EE. UU. y por otros funcionarios gubernamentales en este tipo de estafa.[3]

Tampoco se trata solo de suplantaciones de identidad y de sitios web falsos. Los artículos de noticias, las publicaciones en las redes sociales y los informes y las carteras falsos generados por la IA dan vida a estas ilusiones. La IA puede incluso inflar artificialmente el precio de un activo antes de venderlo, dejando a los inversores en números rojos. A veces, el uso de la IA por parte de los estafadores de inversiones se limita a afirmaciones, aprovechando la reputación de la IA para fundamentar sus mentiras sobre bots comerciales impulsados por la IA y sobre algoritmos avanzados.

6. Estafas de extorsión

Las estafas de extorsión podrían ser las más sucias de los tipos de estafas de la docena sucia contra los adultos mayores. Mientras que otras estafas buscan engañar, las estafas de extorsión se caracterizan por amenazas directas. El estafador afirma tener pruebas que podrían avergonzar o incriminar al adulto mayor, y amenaza con hacer públicas esas pruebas o con compartirlas con los contactos del adulto mayor si este no paga el dinero exigido.

Si bien, en algunos casos, el estafador está haciendo una farsa, en otros verdaderamente ha recopilado información privada para usarla contra su objetivo. Los estafadores que pueden introducir programas maliciosos en la computadora de un adulto mayor pueden grabar pulsaciones de teclas, mirar la cámara web y rastrear un historial en línea que puede ser privado, todo lo cual usarán para chantajear a la víctima. Y como se mencionó anteriormente, los adultos mayores que se encuentran en una estafa romántica podrían ser vulnerables a la sextorsión, donde se los amenaza con publicar imágenes o detalles íntimos si no pagan.

En otras estafas de extorsión, el delincuente se hace pasar por un empleado del Gobierno y alega que el adulto mayor está bajo investigación gubernamental. Exige el pago bajo amenaza de arresto o de procesamiento.

Enfoque en la IA: Si bien la tecnología de la IA se puede utilizar en algunas de las formas más comunes para ayudar a los estafadores a hacerse pasar por funcionarios gubernamentales, otra forma en que se utiliza es para crear pruebas falsas para usar contra los objetivos. Pueden usar la IA generativa para producir videos ultrafalsos o fotos comprometedoras del adulto mayor que puedan usar para extorsionar a la víctima.

7. Estafas de suplantación de agencias gubernamentales

Como se describe en algunos esquemas de extorsión, las estafas de suplantación de agencias gubernamentales se caracterizan por estafadores que se aprovechan de la autoridad de las agencias del Gobierno para asustar a sus víctimas y lograr que les paguen dinero. Estos delincuentes, que generalmente afirman ser del Servicio de Impuestos Internos (IRS), la Administración del Seguro Social (SSA) o Medicare, luego realizan falsas afirmaciones, hacen peticiones y amenazan con consecuencias devastadoras si el adulto mayor no cumple.

Por ejemplo, el falso agente del IRS puede amenazar con arresto o deportación si el adulto mayor no envía dinero para sus supuestos impuestos no pagados. O el falso representante de la SSA puede amenazar con suspender los beneficios del adulto mayor a menos que la persona proporcione información de identificación personal, que luego se utiliza para fines nefastos. Otra trampa común: el agente de seguros de salud impostor recopila tu información personal con el pretexto de ayudarte con tu cobertura de Medicare o de Medicaid.

Una señal de alerta fácil de detectar para esta estafa es que los impostores del Gobierno a menudo exigen el pago mediante tarjetas de débito prepagas, efectivo o transferencias bancarias. También es importante tener en cuenta que, por regla general, las organizaciones gubernamentales no suelen llamarte, enviarte correos electrónicos ni presentarse en tu domicilio. Tampoco te amenazarían ni te solicitarían información personal por correo electrónico.

Enfoque en la IA: Utilizando tecnología especial, los estafadores falsifican el número de teléfono real de una agencia gubernamental o llaman desde el mismo código de área (202 para Washington D. C., por ejemplo). Ver el número de teléfono real de la agencia gubernamental en el identificador de llamadas puede engañarte y hacerte creer que la persona que llama es quien dice ser. Las herramientas de IA también pueden falsificar identificaciones gubernamentales e imitar diseños de correo electrónico oficiales para que el estafador y sus mensajes parezcan más creíbles.

8. Estafas con tarjetas de crédito y cheques

En una época en la que abundan las tarjetas de crédito y las transacciones digitales, el fraude con tarjetas de crédito sigue siendo un método constante para que los estafadores roben dinero. Incluye el robo utilizando no solo tarjetas de crédito, sino también métodos de pago similares, como ACH, EFT y cargos recurrentes.

Los estafadores pueden utilizar tácticas de suplantación de identidad y otros esquemas comunes para obtener acceso a tu número de tarjeta de crédito y a otra información personal identificable que pueda ayudarlos a llevar a cabo este tipo de fraude. En un método, el estafador llama y casi inmediatamente pregunta: "¿Puedes oírme?". Cuando el adulto mayor responde, su “sí” queda grabado y luego se utiliza como verificación de voz para que el estafador autorice cargos en la tarjeta de crédito.

Sin embargo, obtienen la información de la tarjeta de crédito y luego generalmente la exprimen con compras o pueden establecer un cargo recurrente más pequeño que esperan que pase desapercibido. Con suficientes datos personales tuyos, también pueden abrir nuevas líneas de crédito a tu nombre, acumulando una enorme deuda.

Los adultos mayores a menudo son vistos como objetivos atractivos para el fraude con tarjetas de crédito porque muchos tienen buenos puntajes de crédito, ahorros establecidos y un alto nivel de confianza esperado. Y hablando de confianza, si bien muchos de estos tipos de estafas de la docena sucia son cometidos por culpables desconocidos, el fraude con tarjetas de crédito es un delito que a veces también cometen personas que los adultos mayores conocen, incluidos familiares o cuidadores de confianza. Esto hace que sea aún más importante que los adultos mayores protejan su información personal y revisen periódicamente sus cuentas, historial de transacciones y puntajes crediticios.

Enfoque en la IA: Los estafadores utilizarán todo su arsenal de estrategias respaldadas por una combinación de tecnologías de la IA (mensajes con suplantación de identidad avanzados, clonación de voz, videos ultrafalsos y más) para adquirir información personal y de tarjetas de crédito.

9. Estafas de vulneración de correo electrónico empresarial

En 2023, 11.2 millones (19.2 %) de estadounidenses de 65 años en adelante todavía trabajaban o buscaban trabajo activamente.[2] Y los estafadores apuntaban a los adultos mayores en el trabajo a través de estafas de vulneración de correo electrónico comercial, también conocidas como "estafas de vulneración de cuentas de correo electrónico".

Dependiendo del hecho de que la mayoría de las personas confían en el correo electrónico para realizar negocios profesionales, los estafadores envían mensajes de correo electrónico que parecen ser tareas laborales normales de fuentes conocidas, pero la verdad es que es cualquier cosa menos eso. Por ejemplo, el estafador puede enviar una factura por correo electrónico haciéndose pasar por un proveedor con el que tu empresa trabaja habitualmente. Excepto que, esta vez, han enviado un enlace de pago actualizado o quizás una nueva dirección postal para que puedas enviar el cheque.

Eso por sí solo no necesariamente debe ser una señal de alerta cuando todo lo demás en la comunicación parece legítimo. Los estafadores pueden falsificar la cuenta de correo electrónico, el sitio web o el diseño del correo electrónico; o pueden cambiar un detalle pequeño e imperceptible en la dirección de correo electrónico. A primera vista, podría parecer que proviene de una empresa o persona con la que te comunicas habitualmente.

De manera similar, los correos electrónicos de suplantación de identidad son mensajes que parecen provenir de remitentes conocidos y confiables, y manipulan al receptor para que comparta información que de otro modo sería confidencial. Esto ayuda a los ciberdelincuentes a introducirse en las cuentas de la empresa, sus contactos y otra información. Estos correos electrónicos empresariales aparentemente inocentes también pueden engañar a los receptores para que descarguen software malicioso en las computadoras de la empresa, que puede pasar desapercibido.

También ha habido casos en los que el estafador se hace pasar por alguien dentro de la empresa, como el director ejecutivo u otra figura de autoridad. Puede parecer que tu jefe te está pidiendo que emitas un cheque a un proveedor o que compres y envíes tarjetas de regalo a los clientes. Pero, en realidad, la empresa para la que tú trabajas está siendo estafada. Estas estafas son aún más fáciles de llevar a cabo cuando la fuerza laboral de la empresa trabaja de forma remota o existe un entorno de trabajo híbrido que limita las interacciones cara a cara.[4]

Enfoque en la IA: Las capacidades de la IA, que se pueden usar con velocidad, con escala y prácticamente sin costo, han hecho que los estafadores creen estrategias de vulneración de correo electrónico empresarial más elaboradas, de múltiples etapas y canales, que se extienden a mensajes de texto, aplicaciones de comunicación empresarial, llamadas de voz clonadas e incluso llamadas de Zoom ultrafalsas.

10. Estafas de robo de identidad

¿Sabías que tu información personal a menudo es más valiosa que todo el dinero de tu cuenta? Si bien muchas estafas roban dinero en transacciones únicas, las estafas de robo de identidad ponen a la víctima en riesgo repetido, lo que hace que este tipo de fraude sea especialmente insidioso.

Una vez que un estafador obtiene suficiente información de identificación personal (como tu nombre, fecha de nacimiento, número de Seguro Social y contraseñas), generalmente puede obtener acceso a tus cuentas y robar tu seguridad. Peor aún, algunos estafadores usan tu información para abrir nuevas cuentas y acumular asombrosas cantidades de deuda que pueden tardar meses o años en descubrirse y el mismo tiempo en desentrañarse.

Entonces, ¿cómo lo hacen? Con la suplantación de identidad. La suplantación de identidad es una práctica que consiste en hacerse pasar por una fuente confiable, generalmente a través de mensajes como correos electrónicos o mensajes de texto, y solicitar a las personas que revelen información personal y financiera confidencial, como información de identificación, números de tarjetas de crédito y contraseñas. Si bien la IA ha mejorado enormemente la credibilidad de muchos mensajes de suplantación de identidad, hay algunas señales reveladoras que puedes aprender a detectar:

- ofertas que parecen demasiado buenas para ser verdad,
- argumentos de venta de alta presión que enfatizan la urgencia,
- alertas de que hay un problema con tu cuenta,
- enlaces acortados o mal escritos,
- correos electrónicos que no se dirigen a ti por tu nombre,
- mensajes con mala gramática y ortografía,
- solicitudes o exigencias directas de pago,
- solicitudes de confirmación de información personal.

El teléfono sigue siendo el arma favorita cuando apuntan a adultos mayores, y quizás la estafa más frecuente involucra llamadas falsas de telemercadeo. Sin interacción cara a cara y sin rastros documentales, estas estafas son increíblemente difíciles de rastrear. Muchas de estas llamadas comienzan como robollamadas, un mensaje grabado automático que se reproduce cuando respondes el teléfono y que te indica que hables en voz alta o presiones botones para responder preguntas o para conectarte con una persona en vivo. Tu información de contacto puede difundirse fácilmente entre estas organizaciones timadoras, haciendo que el teléfono suene incesantemente.

Registrarte en el Registro Nacional No Llame (DoNotCall.gov) puede ayudar a reducir el número de llamadas de vendedores telefónicos.

Enfoque en la IA: Justo cuando el público se estaba volviendo más consciente de las tácticas de suplantación de identidad y mejoraba su capacidad para reconocerlas, la IA entró en juego y cambió todo. Utilizando información encontrada en Internet, los programas de IA pueden extraer información pública de un objetivo y analizar su comportamiento en línea. Esto permite que la IA produzca campañas de suplantación de identidad personalizadas y altamente específicas que son increíblemente exitosas a la hora de inducir a las personas a revelar información que normalmente protegen. La tecnología de la IA también ha automatizado este proceso, permitiendo a los ciberdelincuentes cometer robos de identidad a mayor escala y a mayor velocidad.

Las leyes a menudo quedan rezagadas ante la tecnología, pero las agencias gubernamentales están trabajando diligentemente para ponerse al día con las estafas integradas con la IA. A principios de 2024, la Comisión Federal de Comunicaciones consideró que todas las llamadas con voces generadas por la IA eran "artificiales" según la Ley de Protección al Consumidor Telefónico. El fallo declaró ilegal la tecnología de clonación de voz utilizada en estafas de robollamadas dirigidas a consumidores y dio a los fiscales generales estatales de todo el país nuevos poderes para procesar las operaciones de robollamadas.[5]

11. Estafas de pagos por adelantado

Las estafas de pagos por adelantado son un juego de dar para recibir, pero debes saber que, si juegas, los estafadores siempre ganan. Utilizando una variedad de enfoques, los delincuentes persuaden a sus víctimas a pagar una cantidad por adelantado después de engañarlas haciéndoles creer que recibirán algo de valor a cambio. Los estafadores a menudo se aprovechan de los deseos y las necesidades básicos, lo que hace más probable que su víctima esté dispuesta a ceder para conseguir lo que necesita. Aquí hay algunos ejemplos:

- **Estafas de alquiler:** Con una alta demanda de viviendas y un inventario bajo, conseguir un lugar asequible para vivir es una tarea difícil en muchas áreas del país y ha estimulado un aumento en las estafas de alquiler. Los estafadores ofrecerán propiedades en alquiler que no les pertenecen o que no están disponibles o no son reales, y exigirán depósitos o tarifas por adelantado para asegurar la propiedad incluso antes de que el inquilino la haya visitado. El falso propietario presiona a los inquilinos interesados para que paguen el anticipo con amenazas de que se verán obligados a ceder el contrato de arrendamiento a una de las muchas otras personas interesadas en él.

- **Estafas de préstamos y de empleo**: Las personas que necesitan ingresos son más susceptibles a las estafas de préstamos y a las estafas de empleo. En el primer caso, los estafadores prometen falsamente préstamos o líneas de crédito para lograr que sus víctimas paguen tarifas por adelantado o un seguro. Para estos últimos, las oportunidades de empleo simuladas requerirán pagos por adelantado para cosas como capacitación de los empleados, verificación de antecedentes, suministros u otros gastos. Solo después de pagar, se descubre que no hay un trabajo real. Los estafadores a menudo adaptan las ofertas de empleo para atraer a los adultos mayores, con promesas de trabajos fáciles para hacer desde casa o beneficios increíbles.

  Algunos estafadores continúan con la farsa hasta después de haber fingido contratarte, aprovechando la oportunidad para obtener tu información de identificación personal como parte de su falsa incorporación. Esta es una de las formas en que los estafadores de pagos por adelantado utilizan su truco más antiguo: la suplantación de identidad para obtener información.

- **Estafas de lotería:** Otro tipo de estafa que consiste en engañar al adulto mayor haciéndole creer que ha ganado dinero o un premio. La Embajada de Estados Unidos en Jamaica recibe informes frecuentes de ciudadanos que pierden dinero debido a fraudes en los pagos por adelantado perpetrados por estafadores en Jamaica. El escenario más frecuente: el estafador hace creer a alguien que ha ganado un sorteo o una lotería, pero que debe pagar tasas o impuestos por adelantado para reclamar el premio o el dinero en efectivo.[6]

Enfoque en la IA: Al igual que con otros tipos de estafas, los estafadores que cobran pagos por adelantado utilizan herramientas de la IA para crear un espejismo de legitimidad para sus reclamos, identidad y ofertas de trabajo. La tecnología de la IA puede extraer datos de bolsas de trabajo y perfiles de LinkedIn para identificar con precisión a los solicitantes de empleo que probablemente muerdan el anzuelo. La IA se puede utilizar para enviar ofertas de empleo falsas, realizar entrevistas automatizadas, recopilar información personal y cobrar tarifas por adelantado.

12. Estafas de ganancias inesperadas

Todo el mundo sueña con ganar a lo grande, pero es posible que termines en la pesadilla real de perder a lo grande si tus ganancias inesperadas resultan ser una estafa. Este tipo de estafa se aprovecha de la esperanza común de ganar dinero (como ganar la lotería o un sorteo, o recibir una herencia inesperada), una esperanza que puede ser especialmente tentadora para los adultos mayores que pueden vivir con un ingreso fijo o limitado.

Por lo general, los estafadores informan a un adulto mayor que ganó la lotería o un sorteo, pero que debe brindar información personal o realizar un pago para desbloquear el premio. A menudo, los adultos mayores reciben un cheque que pueden depositar en su cuenta bancaria, sabiendo que, si bien aparece en su cuenta de inmediato, pasarán algunos días antes de que el cheque falso sea rechazado. Durante ese tiempo, los estafadores cobrarán rápidamente el dinero por supuestas tarifas o impuestos sobre el premio, mientras que a la víctima se le retira el supuesto dinero del premio de su cuenta bancaria tan pronto como el cheque rebota.

En los últimos años, las organizaciones criminales extranjeras, en particular las de Jamaica, se han ganado la reputación de realizar estafas inesperadas. Estos estafadores se hacen pasar por abogados, funcionarios de aduanas o representantes de lotería; y te felicitan por haber ganado un sorteo, una lotería extranjera u otro premio de alto valor. Luego viene el "pero"..., pero primero debes pagar las tarifas de envío, seguro, derechos de aduana o impuestos antes de que puedan liberar tu premio. Estas organizaciones criminales internacionales incluso utilizan mulas de dinero con base en Estados Unidos para que sean intermediarios en sus pagos, lo que hace aún más difícil rastrearlas.[6, 7]

Enfoque en la IA: Los estafadores que buscan obtener ganancias inesperadas emplean muchas de las herramientas de la IA mencionadas anteriormente para hacerse pasar por figuras de autoridad, como abogados u organizaciones conocidas, loterías estatales, o Publishers Clearing House. También utilizan la IA para analizar grandes cantidades de datos demográficos a fin de acercarse con mayor precisión a sus objetivos principales.

Caso de estudio: Una mirada más cercana a las estafas más comunes

Maggie, una viuda de 72 años, conoció a James a través de un sitio de citas en línea para adultos mayores. Rápidamente la cautivó con atención, afecto, grandes gestos y promesas para el futuro. Fue un romance vertiginoso, y ella apenas tuvo tiempo para visitar a sus hijos, asistir a su grupo de la iglesia o dar su caminata diaria con sus vecinos.

En cuestión de unos pocos meses, su relación se volvió más seria, y James convenció a Maggie de invertir una gran suma en una oportunidad lucrativa que, según él, garantizaba su futuro financiero y el de ambos. Sintiéndose presionada, estaba a punto de enviar dinero cuando dudó.

En represalia, James amenazó con exponer mensajes e imágenes íntimos, obtenidos a través de conversaciones manipuladas en línea, a menos que Maggie cumpliera. Temiendo la desgracia, cedió y transfirió el dinero a James. Maggie quedó desconsolada, asustada, en una situación financiera desesperada y sintiéndose muy sola para procesar lo que le sucedió.

- ¿Puedes identificar qué tipo (¡o tipos!) de estafas tuvieron lugar en este escenario?
- ¿Cuáles fueron algunas de las señales de alerta que notaste a medida que avanzaba este escenario?
- ¿Crees que hay algo que Maggie podría haber hecho diferente?

Consejos para evitar estafas

Consejos para evitar estafas de centros de llamadas y de soporte técnico

- No hagas clic en ventanas emergentes, enlaces o archivos adjuntos no solicitados; y no llames a los números de teléfono proporcionados en mensajes de texto o correos electrónicos no solicitados.
- No descargues software de una persona desconocida que se comunicó contigo.
- Nunca permitas que una persona desconocida acceda para ver o controlar tu computadora de forma remota.
- Nunca envíes dinero, criptomonedas o tarjetas de regalo a agentes técnicos o de atención al cliente que se comuniquen contigo sin solicitarlo.
- Nunca compartas tu contraseña u otra información personal con una persona que te contactó sin solicitarlo.
- No te involucres. Está bien eliminar correos electrónicos sin respuesta y simplemente colgar el teléfono.
- Regístrate en el Registro Nacional No Llame (DoNotCall.gov) para reducir el número de llamadas de vendedores telefónicos. También puedes darte de baja de listas de correo múltiples.
- Si tienes problemas reales con la computadora, puedes comunicarte directamente con la compañía de la computadora o del software, o consultar en Better Business Bureau (bbb.org) sobre las empresas locales de soporte técnico de confianza.

Consejos para evitar estafas de violación de datos personales

- No hagas clic en ventanas emergentes, enlaces o archivos adjuntos que te adviertan que tus datos han sido violados.
- Busca señales de alerta, como errores gramaticales y ortográficos, solicitudes para proporcionar o confirmar tu información personal, y presión para actuar rápidamente.
- No respondas a mensajes de texto, correos electrónicos ni llamadas telefónicas que te alerten sobre una violación de datos. En su lugar, comunícate directamente con la empresa mencionada utilizando un número de teléfono o un sitio web confirmados.
- Utiliza contraseñas seguras y habilita la autenticación multifactor para proteger tu información de verdaderas violaciones de datos.

Consejos para evitar estafas de confianza

- Ten en cuenta que el riesgo proviene tanto de los extraños como de las personas cercanas a ti.
- No mezcles las citas con el dinero. Establece límites firmes entre tus finanzas y tus parejas románticas.
- Crea una contraseña familiar secreta para burlar la clonación de voz. Si, alguna vez, un familiar llama pidiendo dinero por una situación urgente, pídele la contraseña para confirmar su identidad.
- Tómate el tiempo para confirmar la identidad de la persona que llama o la situación. Haz preguntas personales que un estafador no pueda responder o cuelga y llama a otro pariente cercano que pueda ayudar a confirmar la situación.
- A los vendedores puerta a puerta o que llamen por teléfono diles siempre: “Nunca compro ni pago a nadie que me llame o me visite sin previo aviso. Envíeme su información por escrito”.
- Para reparaciones del hogar, obtén cotizaciones de varias empresas para confirmar que haya consenso sobre qué trabajo se necesita y asegúrate de obtener un precio justo.
- Nunca pases a la siguiente etapa con un contratista sin un contrato firmado y nunca pagues el total por adelantado. Espera hasta que el trabajo esté completo y pase la inspección.
- Para contratistas, funerarias o cualquier tipo de negocio, asegúrate de que tengan buena reputación llamando a Better Business Bureau al 804-648-0016 o consultando en línea en bbb.org.
- No cedas ante tácticas de venta bajo alta presión. Obtén todo por escrito y tómate tu tiempo para considerar cualquier decisión costosa.
- Considera cuidadosamente a quién le otorgas poderes notariales duraderos e incluye salvaguardas para evitar que tu agente designado los utilice indebidamente.

Consejos para evitar estafas por falta de pago o por falta entrega

- No proporciones información personal o de pago en sitios web desconocidos o no verificados.
- Opta por métodos de pago seguros como tarjetas de crédito que ofrecen protección al comprador.
- Tómate el tiempo para investigar sitios web o vendedores individuales antes de continuar con una compra.
- Verifica la cantidad y el contenido de las valoraciones y las reseñas de los clientes.

Consejos para evitar estafas de inversión

- Ten siempre presente la regla número uno para evitar estafas de inversión: si suena demasiado bueno para ser verdad, ¡probablemente no sea cierto!
- Desconfía de las oportunidades de inversión que prometen cero riesgos, ganancias rápidas o retornos garantizados.
- Ignora las ofertas no solicitadas que piden que inviertas dinero.
- Haz tu tarea para verificar la credibilidad de las oportunidades de inversión y de las personas que las promocionan a partir de múltiples fuentes confiables.
- Consulta con un profesional de inversiones registrado antes de tomar cualquier decisión. Visita Investor.gov para confirmar el estado del registro legalmente obligatorio de los inversionistas y para revisar el historial disciplinario.[3]

Consejos para evitar estafas de extorsión

- Mantén privados los perfiles en línea, como una página de Facebook, de modo que solo puedan verlos las conexiones que apruebes. De la misma manera, solo crea amigos o conéctate en las redes sociales con personas que conozcas y que hayas visto en persona.
- Limita la cantidad de información de identificación personal (como tu fecha de nacimiento, dirección y número de teléfono) que compartes en las redes sociales, perfiles de citas y otros sitios públicos.
- Reconsidera compartir historias demasiado personales en estas plataformas públicas en línea, ya que los extorsionadores podrían usarlas en tu contra.
- Reconsidera seriamente hacer publicaciones, enviar correos electrónicos o mensajes de texto, o compartir fotos o videos íntimos que puedan usarse en estafas de sextorsión.
- Ten en cuenta que un funcionario del Gobierno o un agente de la ley reales no te amenazarán por dinero.
- No entres en pánico: bloquea y denuncia. Los chantajistas cuentan con que te asustarán para que hagas lo que piden. No respondas, no intentes negociar una solución y no pagues. Bloquéalos para que no puedan comunicarse más y denuncia el delito inmediatamente.

Consejos para evitar estafas de suplantación de agencias gubernamentales

- Las agencias gubernamentales nunca te amenazarán con arresto o pérdida de beneficios como consecuencia de no realizar un pago que no hayas confirmado.
- Las agencias gubernamentales nunca te llamarán, enviarán correos electrónicos o mensajes de texto, aparecerán sin previo aviso ni te enviarán mensajes en las redes sociales para solicitarte dinero o información de identificación personal.
- Tienes que saber que el Gobierno nunca te pedirá que pagues mediante transferencia bancaria, tarjetas de regalo, criptomonedas u otros métodos de pago inusuales.
- No confíes en tu identificador de llamadas porque los estafadores pueden falsificar el nombre de una agencia gubernamental o el número de teléfono real cuando llaman.
- No te involucres en estas solicitudes. Siempre puedes comunicarte directamente con la agencia para determinar si existe un problema real o si es necesario tomar alguna medida. Utiliza únicamente números de teléfono verificados que se encuentren en sitios web del Gobierno; nunca llames a un número proporcionado por el contacto original.
- Mantén tu número de Medicare tan privado como tu número de tarjeta de crédito y revisa periódicamente tus estados de cuenta de Medicare.

Consejos para evitar estafas con tarjetas de crédito y cheques

- No hagas clic en nada en un correo electrónico o mensaje de texto no solicitado que te pida que actualices o verifiques la información de la cuenta. Llama al banco o empresa a través de un número verificado para preguntar si la solicitud es legítima.
- Destruye todos los documentos que muestren el número de tu tarjeta de crédito o de tu cuenta bancaria.
- Utiliza el depósito directo para cobrar los cheques de beneficios para evitar que te roben los cheques físicos.
- Nunca proporciones datos personales o de cuentas a alguien que se comunique contigo desde una compañía de tarjetas de crédito. Cuelga y llama directamente a la compañía utilizando el número de teléfono que aparece en tu estado de cuenta o en el reverso de tu tarjeta.
- Protege los inicios de sesión de tu cuenta con contraseñas seguras y habilita la autenticación de dos factores para los inicios de sesión de tu cuenta.
- Utiliza tu tarjeta de débito como si fuera una tarjeta de crédito en las gasolineras para evitar que un dispositivo de clonación te robe el pin.
- Asegúrate de haber configurado todo para recibir alertas de fraude de tu banco y de tu compañía de tarjeta de crédito.

Consejos para evitar estafas de vulneración de correo electrónico empresarial

- Revisa cuidadosamente las facturas y los correos electrónicos que soliciten pagos para confirmar que las direcciones de correo electrónico, los sitios web y los detalles de contactos conocidos sean exactos. Los estafadores cambian detalles menores (por ejemplo, agregan un punto en una dirección de correo electrónico o cambian ".com" por ".co" en un sitio web) para que parezcan correctos.
- Para contactos desconocidos, confirma la validez de la solicitud y de los detalles de pago proporcionados con el departamento de contabilidad de tu empresa.
- Sigue las prácticas seguras de uso del correo electrónico. No abras archivos adjuntos de correo electrónico de remitentes desconocidos y procede con precaución con los archivos adjuntos reenviados.
- Utiliza contraseñas seguras y configura la autenticación de dos o múltiples factores en cualquier inicio de sesión de cuenta empresarial que lo permita.
- Para solicitudes de pago o de compra nuevas o inusuales, verifica su validez en persona o llamando tú mismo a un número confirmado.
- Haz una pausa en cualquier solicitud de pago o de compra en la que sientas que te presionan para actuar rápidamente.

Consejos para evitar estafas de robo de identidad

- Tienes que saber que la meta de un ladrón de identidad es obtener acceso a cuentas bancarias o de otro tipo, líneas de crédito, y demás recursos financieros.
- Sé cauteloso y protege tu información personal dondequiera que se utilice o anote, ya que los ladrones siempre están ideando nuevos métodos para robar tu identidad.
- Nunca compartas tus datos personales o financieros por teléfono o en línea a menos que hayas iniciado la llamada a un número verificado o hayas iniciado sesión en un sitio verificado y seguro.
- Evita conectar tu teléfono o computadora a Internet mediante redes wifi públicas no seguras, ya que esto hace que tu dispositivo sea vulnerable al acceso por parte de ciberdelincuentes.
- Recoge tu correo periódicamente para reducir las posibilidades de que te lo roben (junto con tu identificación personal o con la información de tu cuenta).
- Destruye los documentos que contengan información confidencial de identificación personal o información de cuentas antes de tirarlos a la basura.
- Considera contratar un servicio de monitoreo de robo de identidad con un seguro contra robo de identidad para ayudar a cubrir pérdidas financieras en el peor de los casos.
- Si sospechas que puedes ser víctima de robo de identidad, denúncialo lo antes posible y congela tu crédito con las tres agencias de crédito para evitar que se abran nuevas cuentas a tu nombre.

Consejos para evitar estafas de pagos por adelantado

- Nunca pagues tarifas por adelantado por nada, especialmente por solicitudes de empleo o capacitaciones, por el procesamiento de préstamos, o para reclamar un premio.
- Haz una pausa. Los estafadores te presionan para que actúes rápidamente antes de que tengas tiempo de pensar o de investigar una situación. Nunca pagues una tarifa bajo presión; en lugar de eso, haz una pausa y realiza las diligencias debidas.
- Ten cuidado con las empresas que son difíciles de localizar, que carecen de una dirección física o que no son fácilmente verificables a partir de múltiples fuentes confiables.
- Considera que todas las solicitudes de métodos de pago inusuales son señales de alerta. Estas incluyen transferencias bancarias, tarjetas de regalo y giros postales, todos ellos difíciles de rastrear o de recuperar.
- Si debes pagar una tarifa por adelantado que consideras legítima, utiliza un método de pago seguro y luego controla tus cuentas de cerca.

Consejos para evitar estafas de ganancias inesperadas

- Cabe repetirlo: si suena demasiado bueno para ser verdad, ¡probablemente no sea cierto!
- Recuerda que no puedes ganar si no jugaste. No creas afirmaciones de que ganaste una lotería o un sorteo en los que nunca participaste.
- Los ciudadanos estadounidenses no pueden jugar ni ganar loterías extranjeras. Es ilegal, así que cuelga el teléfono a cualquiera que llame para hablar sobre la lotería de Jamaica o sobre cualquier otra que no hayas jugado.
- Nunca pagues una tarifa por adelantado para reclamar un premio o una herencia. Las loterías y los sorteos legítimos deducen impuestos y tasas del dinero del premio antes de realizar el pago.
- No compartas tu información personal o financiera con nadie que diga necesitarla para confirmar una herencia.

Protégete a ti mismo y a los demás

Ahora que sabes más sobre las estafas más comunes dirigidas a los adultos mayores y cómo evitarlas, puedes compartir ese conocimiento con familiares y amigos que también pueden correr el riesgo de ser un objetivo. También puedes mantenerte atento a señales que indiquen que algún ser querido puede estar sufriendo una estafa financiera u otro problema. A continuación, se muestran algunas señales que debes tener en cuenta:

- Cambios recientes inusuales en cuentas personales, incluidos retiros atípicos, incorporación de nuevas personas o uso repentino de una tarjeta de débito o crédito.
- Una persona de repente parece confundida, descuidada o temerosa.
- Un cuidador que no permite que otros accedan a un adulto mayor.
- Acumulación de correos de sorteos, suscripciones a revistas u "obsequios" que indican que el nombre de la persona se ha agregado a una lista.

Denunciar estafas y otros pasos para víctimas de fraude financiero

Cómo denunciar estafas financieras

Los adultos mayores deben denunciar las estafas relacionadas con las finanzas a la Línea Directa Nacional contra el Fraude a Personas Mayores o presentar una queja ante el IC3 del FBI. A continuación, se detallan estos y otros recursos para denunciar:

- Línea Directa Nacional contra el Fraude a Personas Mayores: 833-FRAUD-11 (833-372-8311)
- IC3 del FBI: ic3.gov
- Comisión Federal de Comercio: ReportFraud.ftc.gov
- Servicios de Protección para Adultos: napsa-Now.org/Help-in-Your-Area
- Medicare: 800-MEDICARE

Otras medidas inteligentes que puedes tomar

- Comunícate con todos tus bancos y compañías de tarjetas de crédito de inmediato.
- Cancela cualquier tarjeta de débito o crédito vinculada a la cuenta robada. Restablece los números de identificación personal (pines) y las contraseñas.
- Envía una alerta de fraude a las tres agencias de informes crediticios (Experian, Equifax y TransUnion) y considera congelar tu crédito.
- Presenta una denuncia a la policía. Es posible que la policía no pueda hacer mucho, pero quizá necesites una denuncia policial para resolver el problema.

Recursos útiles

Programa de Servicios Legales para Estadounidenses Mayores de la Administración para la Vida Comunitaria
acl.gov/Programs/Legal-Help/Legal-Services-Elderly-Program

Recursos para adultos mayores de Better Business Bureau
804-780-2222
bbb.org/All/Older-Adult-Resources

Oficina para la Protección Financiera del Consumidor
ConsumerFinance.gov/Consumer-Tools/Educator-Tools/Resources-for-Older-Adults/

Centro Nacional de Abuso de Adultos Mayores
ncea.acl.gov

Centro Nacional de Leyes y Derechos de Adultos Mayores
ncler.acl.gov

Consejo Nacional para Adultos Mayores
ncoa.org

Patrulla Medicare para Personas Mayores
smpResource.org

Denuncias de fraude de Seguro Social
800-269-0271
oig.ssa.gov

Localizador de Servicios de Protección para Adultos por estado
napsa-Now.org/Help-in-Your-Area/

Apéndice A

Fiscales generales: Estados

Alabama
334-242-7300

Alaska
907-269-5100

Arizona
602-542-5025

Arkansas
800-482-8982

California
916-445-9555

Colorado
720-508-6000

Connecticut
860-808-5420

Delaware
302-577-8600

Florida
850-414-3300

Georgia
404-651-8600

Hawái
808-586-1500

Idaho
208-334-2400

Illinois
312-814-3000

Indiana
317-232-6330

Iowa
515-281-5044

Kansas
785-296-3751

Kentucky
502-696-5300

Luisiana
225-326-6465

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
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

Ohio
614-466-4986

Oklahoma
405-521-3921

Oregón
503-378-4400

Pensilvania
717-787-3391

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

Utah
800-244-4636

Vermont
800-649-2424

Virginia
804-786-2071

Washington
360-753-6200

Virginia Occidental
304-558-2021

Wisconsin
608-266-1221

Wyoming
307-777-7841

Fiscales generales: Territorios

Samoa Americana
684-633-4163

Distrito de Columbia
202-442-9828

Guam
671-475-2720

Islas Marianas del Norte
670-237-7600

Puerto Rico
787-721-2900

Islas Vírgenes de EE. UU.
340-774-5666

Fuentes

1. Informe de fraude a personas mayores de 2023, Centro de Denuncias de Delitos en Internet, Oficina Federal de Investigaciones.
https://www.ic3.gov/AnnualReport/Reports/2023_IC3ElderFraudReport.pdf

2. Perfil de las personas mayores estadounidenses de 2023, Administración para la Vida Comunitaria.
https://acl.gov/sites/default/files/Profile%20of%20OA/ACL_ProfileOlderAmericans2023_508.pdf

3. Inteligencia artificial y fraude de inversión, Departamento de Seguros, Valores y Banca de D. C.
https://disb.dc.gov/page/artificial-intelligence-ai-and-investment-fraud

4. Guía contra la suplantación de identidad: Detener el ciclo de ataque en la fase uno, Agencia de Seguridad Nacional, 2023.
https://media.defense.gov/2023/Oct/18/2003322402/-1/-1/0/CSI-PHISHING-GUIDANCE.PDF

5. Resolución declaratoria, Comisión Federal de Comunicaciones, 2024.
https://docs.fcc.gov/public/attachments/FCC-24-17A1.pdf

6. Estafas de lotería, Embajada de Estados Unidos en Jamaica.
https://jm.usembassy.gov/lottery-scams/?_ga=2.158491258.19693272.1674836526-841878856.1674836526

7. Alerta de estafa para personas mayores, Departamento de Justicia de EE. UU.
https://www.justice.gov/elderjustice/senior-scam-alert

Notas

national council on aging®

@NCOAging | ncoa.org
251 18th Street South, Suite 500, Arlington, VA 22202