



BOLETÍN DE NOTICIAS DEL CONSUMIDOR DE LA FLORIDA

Enero 2025

Una Publicación del Departamento de
Agricultura y Servicios al Consumidor

INICIO DE LA TEMPORADA DE IMPUESTOS

El Formulario W-2 del IRS, también conocido como “Declaración de Salarios e Impuestos”, señala el comienzo de la temporada de impuestos y es el formulario que a la mayoría de las personas les importa cuando se preparan para presentar sus impuestos federales. El formulario muestra la cantidad de dinero que ganó y la cantidad de impuestos retenidos de sus cheques de pago, así como los beneficios proporcionados durante el año anterior y cuánto contribuyó a su plan de jubilación durante el año. La información del Formulario W-2 se utiliza cuando presenta sus declaraciones de impuestos personales, tanto federales como estatales, ante el IRS y la agencia tributaria de su estado, y para calcular los beneficios del Seguro Social y Medicare.

Los empleadores deben proporcionar a los empleados una copia del Formulario W-2 antes del 31 de enero de cada año. Estos formularios se pueden enviar en papel o en formato digital y se consideran a tiempo si se dirigen correctamente y se envían por correo antes del 31 de enero.

El robo de identidad es una preocupación real a la hora de declarar impuestos. Los contribuyentes que presentan su declaración a través de dispositivos móviles, tabletas y aplicaciones que utilizan redes inalámbricas compartidas corren un mayor riesgo de que su identidad tributaria se vea comprometida. Proteger la información personal y los números de Seguro Social durante todo el año es el paso más importante para salvaguardar la identidad de una persona. Aparte de eso, presentar una declaración de impuestos lo antes posible es lo mejor que puede hacer para prevenir el robo de identidad relacionado con los impuestos.

El Servicio de Impuestos Internos no verifica la validez de los formularios de impuestos individuales. La agencia solo se da cuenta de los problemas cuando se presentan dos declaraciones utilizando el mismo número de Seguro Social. Si un ladrón de identidad tiene la información correcta, puede presentar una declaración de impuestos fraudulenta a partir del 20 de enero y vencer a un contribuyente legítimo para obtener su reembolso.

El [Federal Trade Commission](#) recomienda los siguientes pasos para ayudar a prevenir el robo de identidad relacionado con los impuestos:

- Use una conexión segura a Internet si presenta su declaración electrónicamente, o si presenta una copia impresa, envíe su declaración de impuestos directamente desde la oficina de correos.
- Destruye copias de su declaración de impuestos, borradores u hojas de cálculo que ya no necesites.
- Responda a todo el correo del IRS lo más pronto posible.
- No de su número de Seguro Social a menos que sea necesario.
- Investigue a fondo a un preparador de impuestos antes de entregar información personal.
- Revise su informe de crédito al menos una vez al año de forma gratuita para asegurarse de que no se hayan abierto otras cuentas a su nombre.

www.FloridaConsumerHelp.com

1-800-HELP-FLA(435-7352) • Mon-Fri, 8a.m. – 5p.m., EST • 1-800-FL-AYUDA(352-9832)

Si usted es víctima de robo de identidad, la Comisión Federal de Comercio recomienda estos pasos:

- Presente una queja ante la FTC en identitytheft.gov.
- Comuníquese con una de las tres principales agencias de crédito para colocar una “alerta de fraude” en tus registros de crédito:
 - o www.Equifax.com 1-800-525-6285
 - o www.Experian.com 1-888-397-3742
 - o www.TransUnion.com 1-800-680-7289
- Cierre cualquier cuenta financiera o de crédito abierta por ladrones de identidad.

Si su número de Seguro Social está comprometido y sabe o sospecha que es víctima de robo de identidad relacionado con los impuestos, el IRS recomienda estos pasos adicionales:

- Responder inmediatamente a cualquier aviso del IRS; Llame al número proporcionado.
- Complete el Formulario 14039 del IRS, Declaración Jurada de Robo de Identidad, si su declaración electrónica es rechazada debido a una presentación duplicada bajo su SSN o si se le indica que lo haga. Use un formulario rellenable en IRS.gov, imprima y luego adjunte el formulario a su declaración impresa y envíelo por correo de acuerdo con las instrucciones.
- Continúe pagando sus impuestos y presente su declaración de impuestos, incluso si debe hacerlo en papel.
- Si anteriormente se comunicó con el IRS y no tenía una resolución, comuníquese con nosotros para obtener asistencia especializada al 1-800-908-4490. Tenemos equipos disponibles para ayudar.

Más información disponible en: IRS.gov/identitytheft o de la [FTC identitytheft.gov](http://FTC.identitytheft.gov).



EVITE UN AUTOMÓVIL USADO DAÑADO POR UNA INUNDACIÓN

CARFAX, una empresa que proporciona informes del historial de vehículos para automóviles y camiones en los Estados Unidos ha estimado que 347,000 automóviles sufrieron daños por inundaciones durante la temporada de huracanes de 2024. Aproximadamente 120,000 vehículos en Florida resultaron dañados durante el huracán Milton, y otros 138,000 vehículos se vieron afectados por el huracán Helene en varios estados. Si bien el huracán Debby causó inundaciones generalizadas en las regiones de Big Bend, no está disponible una fecha específica sobre el número de automóviles dañados por esa tormenta.

A los autos inundados generalmente se les otorga un nuevo título llamado "título de salvamento". Esto ocurre cuando el vehículo ha sido considerado una pérdida total por una compañía de seguros debido a un daño significativo y el costo de repararlo excederá su valor de mercado. Un título de salvamento esencialmente marca un vehículo como gravemente dañado y no se puede conducir legalmente a menos que se reconstruya e inspeccione para cumplir con los estándares estatales.

Los vendedores sin escrúpulos pueden tratar de ocultar el verdadero historial de un vehículo y defraudar a los compradores mediante el "lavado de títulos". Esta es la práctica ilegal de eliminar información, como daños por inundación, del título de un automóvil para facilitar la venta del vehículo mediante la presentación de un título "limpio". A menudo, estos vehículos se transportan fuera del área de inundación a lugares donde los compradores pueden estar menos conscientes de las señales de advertencia de daños por inundación.

Es posible que los compradores no sepan que un automóvil está dañado a menos que lo miren de cerca o lo inspeccionen. La Comisión Federal de Comercio (FTC, por sus siglas en inglés) recomienda seguir estos pasos al comprar un vehículo usado:

Verifique si hay signos y olores de daños por inundación. ¿Hay barro o arena debajo de los asientos o el tablero? ¿Hay óxido alrededor de las puertas? ¿La alfombra está suelta, manchada o desparejada? ¿Hueles a moho o descomposición, o a productos de limpieza fuertes, en el auto o en el maletero?

Verifique si hay antecedentes de daños por inundación. El [National Insurance Crime Bureau's](#) (NCIB) La base de datos gratuita mostrará si un automóvil fue dañado por una inundación, robado, pero no recuperado, o declarado como rescatado, pero solo si el automóvil estaba asegurado cuando se dañó.

Obtén un informe del historial del vehículo. Comience en [vehiclehistory.gov](#) para obtener información gratuita sobre el título de un vehículo, la lectura más reciente del odómetro y la condición. Por una tarifa, puede obtener otros informes con información adicional, como el historial de accidentes y reparaciones. La FTC no respalda ningún servicio específico. Más información en [ftc.gov/usedcars](#).

Obtenga ayuda de un mecánico independiente. Un mecánico puede inspeccionar el automóvil en busca de daños por agua que pueden destruir lentamente los sistemas mecánicos y eléctricos y causar óxido y corrosión.

Denuncie el fraude. Si sospecha que un concesionario está vendiendo a sabiendas un automóvil dañado por la tormenta o un vehículo recuperado como un automóvil usado en buenas condiciones, comuníquese con la [NICB](#). También infórmele a la FTC en [ReportFraud.ftc.gov](#) y al [fiscal general de su estado](#).



ESTAFAS DE TAREAS LABORALES

Por Jim Kreidler, Especialista en Educación del Consumidor, FTC

¿Has recibido mensajes inesperados sobre el trabajo en línea? El nuevo programa de la FTC [Data Spotlight](#) destaca un gran aumento en el número de personas que informan sobre la [estafas laborales](#), o “estafas de tareas”. Sigue leyendo para saber qué son y cómo evitarlos.

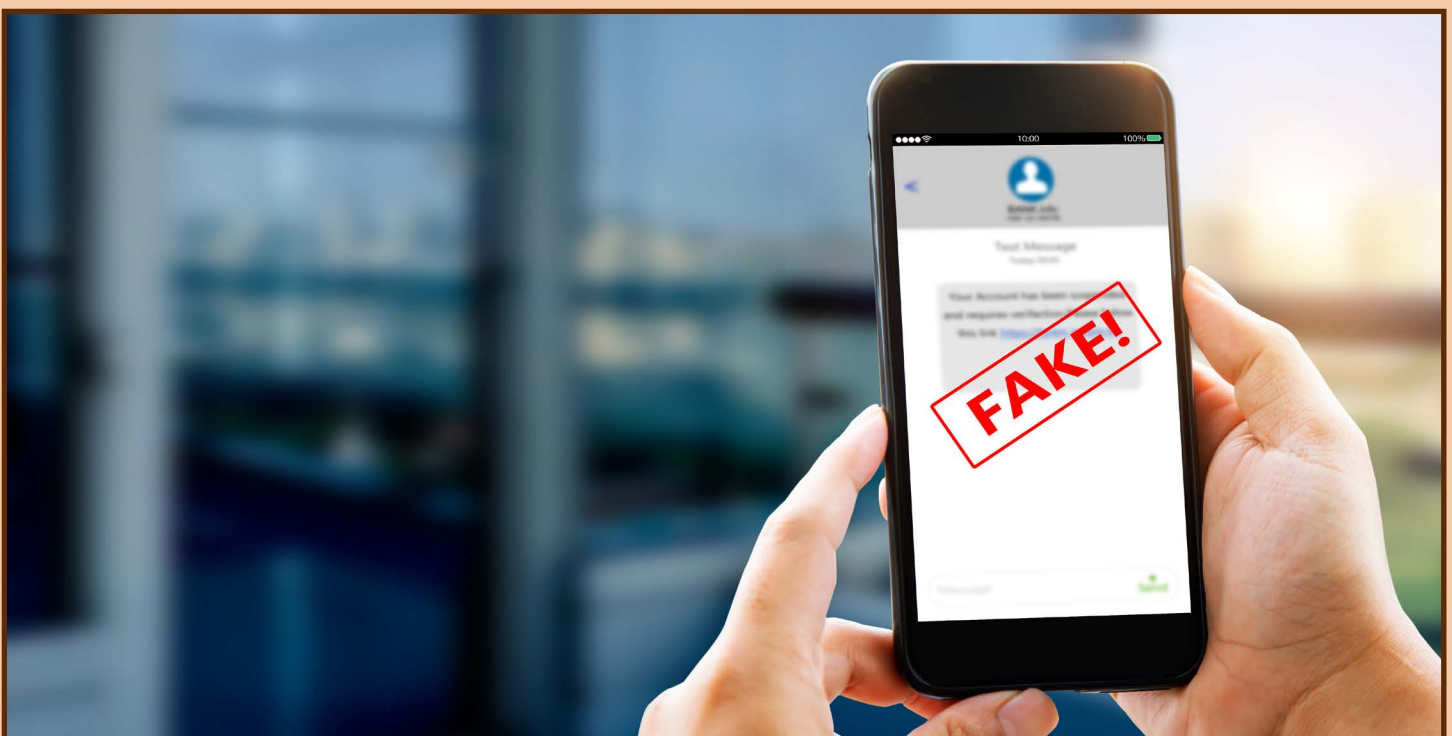
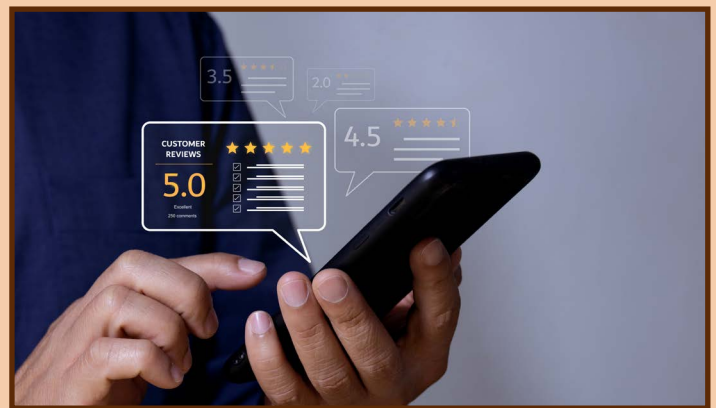
En una estafa de tareas, los estafadores le piden que realice tareas simples y repetitivas, como dar me gusta a los videos o calificar imágenes de productos en línea. El supuesto “trabajo” consiste en completar tareas en una aplicación o plataforma online por las que “ganarás dinero” con una “comisión” con cada clic. Pero esas promesas son falsas: no hay comisiones y nadie más que los estafadores ganan dinero.

Las estafas de tareas generalmente comienzan con un mensaje de texto inesperado que ofrece trabajo en línea. Dicen que se puede “ganar mucho dinero” “impulsando productos” o haciendo “tareas de optimización” en línea. Una vez que completes cada tarea, verás un recuento cada vez mayor de supuestas ganancias en la aplicación (son falsas). En algún momento, la aplicación o la plataforma en línea te pedirá que deposites tu propio dinero, generalmente en criptomonedas, para completar tu próximo conjunto de tareas y para sacar tus supuestas ganancias (falsas) de la aplicación. Pero si realiza el depósito, no solo se perderá su dinero real, sino que nunca obtendrá esas ganancias falsas.

Para detectar y evitar estafas de tareas:

- Ignora los mensajes de texto genéricos e inesperados o los mensajes de WhatsApp sobre trabajos. Los empleadores reales nunca se comunicarán con usted de esa manera.
- Nunca le pagues a nadie para que le paguen o para que consigas un trabajo. Esa es una señal segura de una estafa.
- No confíes en nadie que diga que te pagará por calificar o dar me gusta a las cosas en línea. Eso es ilegal y ninguna empresa honesta lo hará.

Obtenga más información sobre cómo detectar y evitar estafas en ftc.gov/scams y denuncie las estafas a la FTC en ReportFraud.ftc.gov.



FRAUDE EN HOSPICIOS CUIDADOS PALIATIVOS

Por Kira Krown, Especialista en Educación del Consumidor, FTC

¿Alguien se acercó y le ofreció beneficios gratuitos en el hogar, como cocinar y limpiar, a cambio de su número de Medicare? No lo des. Podría tratarse de un estafador que intenta cometer fraude de hospicio.

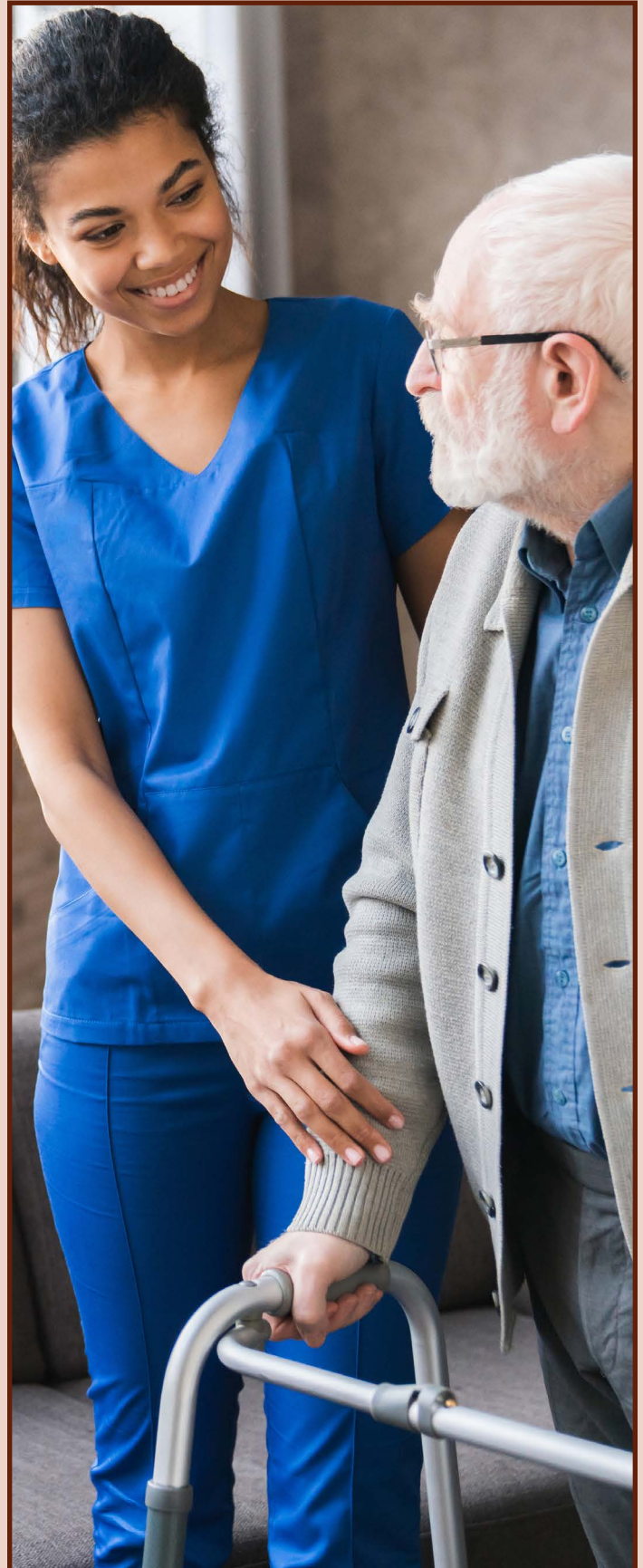
Los estafadores se dirigen a los adultos mayores, con llamadas, mensajes de texto, correos electrónicos, anuncios falsos e incluso visitas puerta a puerta, afirmando que le ofrecerán servicios como cocina, limpieza y atención médica en el hogar gratis. Lo que probablemente no te dirán es cómo: Quieren [cometer fraude](#) al inscribirlo en el cuidado de hospicio de Medicare, así es, hospicio. Luego, pueden facturar a Medicare por todo tipo de servicios en su nombre.

Esto es lo que debe saber: Los cuidados paliativos son un servicio especializado, que a menudo se realiza en el hogar, para personas con una enfermedad terminal que se acerca al final de la vida. Solo su médico puede certificar que usted es elegible para el hospicio (lo que significa que su esperanza de vida es de 6 meses o menos). Si se inscribió en un programa de hospicio y no lo necesita, esto podría afectar su cobertura de Medicare en el futuro. Cualquiera que le diga lo contrario es un estafador.

Estas son algunas maneras de evitar las estafas de hospicio:

- Nunca le dé su número de Medicare a alguien que ofrezca servicios “gratuitos” como limpieza o cocina. Medicare no ofrece servicios gratuitos como ese.
- Nunca acepte inscribirse en cuidados paliativos a cambio de beneficios o regalos como dinero, tarjetas de regalo o comestibles.
- Sepa que Medicare nunca irá a su casa para inscribirlo en los servicios. Si alguien llama a su puerta, dice que es de Medicare e intenta que se inscriba en los servicios, está mintiendo. No les des ninguna información.

Si cree que ha detectado o experimentado un fraude en un hospicio, repórtelo lo antes posible. Llame al 1-800-MEDICARE o comuníquese con su [Patrulla de Medicare para Personas Mayores local](#) para obtener ayuda. Más información en [Medicare.gov/fraud](https://www.medicare.gov/fraud).



ESTAFAS DE PHISHING

Por Ari Lazarus, Especialista en Educación del Consumidor, FTC

A los estafadores les encanta un buen disfraz. Un día aparecen enviándote un mensaje de texto sobre una [entrega que te perdiste](#), al siguiente dicen que necesitas solucionar un [problema con tu cuenta de Netflix](#). A continuación, le indicamos cómo evitar estas estafas de phishing.

[Los correos electrónicos y mensajes de texto de phishing](#) a menudo cuentan una historia para engañarlo para que haga clic en un enlace o abra un archivo adjunto. Tal vez sea un correo electrónico o un mensaje de texto inesperado que se hace pasar por una empresa que conoces o en la que confías, como una empresa de servicios públicos que te pide que realices un pago. O tal vez sea una invitación inesperada a una fiesta que parece ser de un amigo o familiar.

No hagas clic en enlaces ni descargues archivos adjuntos en estos mensajes. Puede dar lugar a una solicitud de información personal, como su número de Seguro Social, tarjeta de crédito o cuenta bancaria, y robo de [identidad](#). O bien, el enlace o archivo adjunto podría descargar [malware dañino](#) en su dispositivo.

¿Cómo puedes detectar estas estafas? Si recibes un correo electrónico o un mensaje de texto en el que se te pide que hagas clic en un enlace o abras un archivo adjunto, pregúntate:

¿Tengo una cuenta en la empresa o conozco a la persona que se puso en contacto conmigo?

- **Si la respuesta es “No”**, es probable que se trate de una estafa de phishing. Si bien las empresas reales pueden comunicarse con usted por correo electrónico, las empresas legítimas no enviarán un correo electrónico o un mensaje de texto inesperado con un enlace para actualizar su pago o información de cuenta. Para conocer otros signos de phishing, consulte [Cómo reconocer el phishing](#).
- **Si la respuesta es “Sí”**, comuníquese con la compañía usando un número de teléfono o un sitio web que sepa que es real, no la información en el correo electrónico. O comuníquese con tu amigo directamente en un correo electrónico o mensaje de texto separado para confirmar que realmente es él. Entenderán si sospechas de esa invitación inesperada para hacer clic en un enlace.

Reenvíe correos electrónicos de phishing a reportphishing@apwg.org (una dirección utilizada por el Grupo de trabajo antiphishing, que incluye ISP, proveedores de seguridad, instituciones financieras y agencias de aplicación de la ley). Informe a la empresa o persona que se hizo suplantar sobre el esquema de phishing. Y repórtelo a la FTC en www.FTC.gov/Complaint.



CORREO ELECTRÓNICO O REDES SOCIALES HACKEADOS

Por Álvaro Puig, Especialista en Educación del Consumidor, FTC

Los piratas informáticos se dirigen a sus cuentas de correo electrónico y redes sociales para robar su información personal. Como su nombre de usuario y contraseña, números de cuenta bancaria o de tarjeta de crédito, o número de Seguro Social. Si lo consiguen, lo utilizan para cometer [robo de identidad](#), propagar malware o estafar a otras personas. Entonces, ¿cuáles son las señales de que alguien hackeó tu cuenta y cómo puedes recuperar una cuenta robada?

Estas son algunas cosas que podrían indicarle un problema:

- Recibes una notificación de que tu dirección de correo electrónico o número de teléfono han cambiado. O que se restableció su contraseña. Pero tú no hiciste esos cambios.
- Recibes un mensaje de que alguien intentó iniciar sesión, o inició sesión, y no fuiste tú.
- No puedes iniciar sesión en tu cuenta.

Si **no puede** iniciar sesión en tu cuenta, sigue las instrucciones de recuperación de cuenta del proveedor. Aquí hay enlaces a algunos de ellos.

Facebook	Microsoft	WhatsApp
Google	Pinterest	X
Instagram	Reddit	Yahoo
Linkedin	Snapchat	YouTube

Si recibes una notificación sobre una actividad que no reconoces y puedes iniciar sesión, esto es lo que **debe** hacer:

Cambia la contraseña de tu cuenta. Cree [una contraseña única y segura](#) que sea difícil de adivinar. Apunta a 12 a 15 caracteres. O usa una frase de contraseña, una serie de palabras separadas por espacios. A continuación, cierre la sesión de esa cuenta en todos los dispositivos. De esa manera, cualquier persona que haya iniciado sesión en su cuenta en otro dispositivo será expulsada.

Protege tu cuenta. Si la cuenta ofrece [autenticación de dos factores](#) (2FA), actívala para agregar una capa adicional de seguridad. De esa manera, un pirata informático con su contraseña no puede iniciar sesión en su cuenta sin un segundo factor de autenticación. Como un código de verificación que se obtiene por mensaje de texto o correo electrónico, o desde una aplicación de autenticación.

Actualiza la información de recuperación de tu cuenta. La información de recuperación de la cuenta te ayuda a volver a acceder a tu cuenta si estás bloqueado, has olvidado tu contraseña o si otra persona la está usando. Verifique la información de recuperación de su cuenta y asegúrese de que la dirección de correo electrónico y el número de teléfono que figuran sean correctos.

Comprueba si hay señales de que alguien ha tenido acceso a tu cuenta. Comprueba si hay reglas de reenvío automático en tu cuenta de correo electrónico que no hayas configurado. Los piratas informáticos pueden crear estas reglas para reenviar sus correos electrónicos a otra dirección. Revisa tus redes sociales para ver si hay mensajes que el hacker publicó o envió, o si hay nuevos amigos que no reconozcas.

Si crees que alguien robó tu información personal, ve a [IdentityTheft.gov](#) para reportarlo y obtener un plan de recuperación personalizado.

ACERCA DE LA DIVISIÓN FDACS DE SERVICIOS AL CONSUMIDOR

FDACS es la agencia estatal de protección al consumidor de Florida responsable de manejar las quejas de los consumidores y regular muchas industrias que afectan directamente a los consumidores de Florida. FDACS maneja más de 400,000 quejas y consultas de los consumidores, supervisa más de 500,000 dispositivos regulados, entidades y productos como bombas de gas y básculas de comestibles, realiza más de \$30,000 análisis de laboratorio en productos como gasolina y fluido de freno, realiza casi 9,000 inspecciones de paseo justo y devuelve más de \$2.8 millones a los consumidores a través de mediaciones con empresas.



La División de Seguridad Alimentaria supervisa los alimentos desde el punto de fabricación y distribución a través de las ventas al por mayor y al por menor para garantizar al público productos alimenticios seguros, saludables y debidamente representados.

OPRIMA EN EL ICONO ANTERIOR PARA VER LO RETIRADO, LOS RETIROS DEL MERCADO Y LAS ALERTAS DE SEGURIDAD



La Comisión de Seguridad de Productos de Consumo proporciona información sobre la retirada de productos de consumo como parte de la misión de la agencia de proteger a los consumidores y a las familias de los productos peligrosos.

OPRIMA EN EL ICONO ANTERIOR PARA VER LO RETIRADO, LOS RETIROS DEL MERCADO Y LAS ALERTAS DE SEGURIDAD.

El Departamento de Agricultura y Servicios al Consumidor de Florida es el centro de intercambio de información del estado para quejas, protección e información de los consumidores. Los consumidores que deseen información sobre la presentación de una queja contra una empresa o que crean que se ha producido fraude pueden visitarnos en línea en FloridaConsumerHelp.com o ponerse en contacto con la línea directa de información y protección al consumidor del departamento llamando al 1-800-HELP-FLA (435-7352) o al 1-800-FL-AYUDA (352-9832) en español.