



BOLETÍN DE NOTICIAS DEL CONSUMIDOR DE LA FLORIDA

Febrero 2020

www.FDACS.gov

**435-7352
1-800-HELP-FLA**

**352-9832
1-800-FL-AYUDA**

Robo de identidad relacionado con impuestos

Un ladrón de identidad puede usar su número de Seguro Social (SSN) para obtener un reembolso de impuestos o un trabajo. Esto es robo de identidad relacionado con impuestos. Es posible que no sepa que ha sucedido hasta:

- El IRS le envía una carta por correo diciendo que han recibido una declaración de impuestos sospechosa que usa su SSN, o
- Intenta presentar su declaración por correo electrónico, pero se rechaza como un duplicado porque una devolución ya se ha archivado utilizando su SSN.

Si el IRS le envía una carta, siga las instrucciones de la carta. Luego visite [IdentityTheft.gov](https://www.identitytheft.gov) para reportar el robo de identidad tanto al IRS como a la FTC y obtenga un plan de recuperación.



Florida Department of Agriculture and Consumer Services

Descubrir el robo de identidad relacionado con los impuestos

Si alguien usa su SSN para solicitar un reembolso de impuestos antes de que usted lo haga, esto es lo que sucede: Cuando usted presenta su declaración, los registros del IRS mostrarán que otra persona ya ha presentado y recibido un reembolso. Si usted presenta por correo, el IRS le enviará un aviso o carta por correo diciendo que se presentó más de una declaración para usted. Si intenta presentar electrónicamente, el IRS rechazará su declaración de impuestos como una presentación duplicada.



Si alguien usa su SSN para obtener un trabajo, el empleador puede reportar los ingresos de esa persona al IRS usando su SSN. Cuando presenta su declaración de impuestos, no habría incluido esos ingresos. Los registros del IRS mostrarán que usted no reportó todos sus ingresos. La agencia le enviará un aviso diciendo que tenía salarios que no reportó. Pero el IRS no sabe que esos salarios fueron reportados por un empleador que usted no conoce, por el trabajo realizado por otra persona.

Los avisos del IRS sobre el robo de identidad relacionado con impuestos se envían por correo. El IRS no inicia contacto con un contribuyente enviando un correo electrónico, texto o mensaje de redes sociales que solicita información personal o financiera. El IRS tampoco llama a los contribuyentes con amenazas de demandas o arrestos. Y, el IRS nunca le pedirá que envíe dinero, pague con una tarjeta de regalo o tarjeta de débito prepagada, o comparta la información de su tarjeta de crédito por teléfono.

Si recibe un correo electrónico, texto u otro mensaje electrónico que dice ser del IRS, no responda ni haga clic en ningún enlace. En su lugar, reenvíelo a phishing@irs.gov. E informe a los impostores del IRS al Inspector General del Tesoro de los Estados Unidos para la Administración Tributaria en [tigta.gov](https://www.tigta.gov).



Tratar con el Robo de Identidad Relacionado con Impuestos

Si el IRS le envía un aviso o carta diciendo que alguien usó su SSN para obtener un reembolso de impuestos, o diciendo que hay otro problema, responda rápidamente y siga las instrucciones en la carta.

- Llame al IRS usando el número de teléfono que aparece en la carta. Necesitará la carta y una copia de la declaración de impuestos de su año anterior cuando llame para ayudar a verificar su identidad. Visite la guía del IRS, Asistencia para Víctimas de Robo de Identidad del [IRS: Cómo funciona](#), para obtener más información.



Si cree que alguien usó su SSN para solicitar un reembolso de impuestos, pero no ha recibido una carta del IRS, use [IdentityTheft.gov](#) para reportarlo al IRS y FTC y obtener un plan de recuperación.

- Visite [IdentityTheft.gov](#) para completar una [Declaración Jurada](#) de Robo de Identidad del IRS (Formulario 14039) del IRS y enviarla al IRS en línea para que el IRS pueda comenzar a resolver su caso. También estará reportando el robo de identidad a la FTC.
- Presente su declaración de impuestos y pague los impuestos que debe. Si no puede presentar su declaración de impuestos por correo electrónico, es posible que deba enviar una declaración en papel por correo.

Otros pasos para reparar el robo de identidad

A continuación, es importante limitar el daño potencial causado por el robo de identidad.

- Ponga una [alerta de fraude](#) en sus informes de crédito.
- [Solicite sus informes de crédito gratuitos](#) y cierre las nuevas cuentas abiertas a su nombre.
- Considere la posibilidad de poner un [congelando](#) de crédito en sus informes de crédito.

Visite [IdentityTheft.gov](#) para obtener ayuda con estos pasos importantes.



Revisión del crimen de identidad



2019 fue un gran año para la delincuencia de identidad, que incluye estafas, fraude, violaciones de datos, ciberdelincuencia, y todos los otros tipos de delitos que van con él. Los usuarios de la tecnología todavía están sintiendo las secuelas de cosas como la debacle de privacidad de [Facebook/Cambridge Analytica](#) que se descubrió el año pasado, y el Congreso todavía está en juego sobre qué hacer con la privacidad de los consumidores en la era de las redes sociales. Además, el hecho de que los ataques de phishing se hubieran más que [duplicado en 2018 durante](#) el año anterior, los investigadores, las empresas, los legisladores y los consumidores por igual habían prestado más atención a los mensajes que reciben.

Afortunadamente, llegó una nueva legislación para hacer que las vidas de privacidad de los consumidores sean un poco más seguras. El Reglamento General de Protección de Datos (RGPD), una ley de privacidad de datos que cambia el juego entró en vigor en Europa en 2018 infligiendo sanciones estrictas a las empresas que recopilan y almacenan datos, pero dejan que caigan en manos equivocadas. Pronto entrarán en vigor nuevas leyes con el fin de fortalecer la [privacidad](#) y la elección del consumidor en California [y Colorado](#). Lo mejor de todo es que la conciencia de lo que constituye este tipo de crímenes y cómo reconocerlos está aumentando.



Sin embargo, esta noticia de bienvenida no significa que los consumidores son completamente seguros o que los piratas informáticos finalmente se están rindiendo. Con cada nueva plataforma, herramienta o tecnología, hay un potencial aún mayor para nuevas vías de ataque. Los proveedores de atención médica y las compañías de seguros continuaron siendo [uno de los objetivos más afectados](#) en 2019, gracias a la abrumadora cantidad de información de identificación personal (PII) que recopilan. Las infracciones de “[exposición](#) accidental”, que pueden ocurrir cuando las empresas almacenan enormes bases de datos de información privada en un servidor en línea, pero no lo conocen, fueron un delito de identidad común de 2019 para las empresas de renombre. Incluso el entretenimiento no era seguro, ya que muchas [aplicaciones y portales](#) de juegos en línea sufrieron violaciones de datos que se rastrearon para reutilizar contraseñas en varios sitios.



2019 no sólo vio una gran cantidad de grandes violaciones de datos, sino también acuerdos en casos de violación de datos, así.

- **Acuerdo de Equifax:** En julio, [Equifax llegó a un acuerdo de \\$700 millones](#) por los daños causados por su violación de datos. Equifax acordó gastar \$425 millones para ayudar a las víctimas de la violación, lo que llevó a varias discusiones sobre [cómo presentar una reclamación](#).
- **Acuerdo de Facebook:** Mientras que el acuerdo Equifax era el más grande en la historia de las violaciones de datos en ese momento, Facebook lo superó sólo dos días después, ya [que se les ordenó pagar 5.000 millones de dólares](#). Después de la liquidación, Facebook dijo que requería un “cambio fundamental” en el enfoque de Facebook a todos los niveles de la compañía en términos de su privacidad.
- **Acuerdo de Yahoo!:** Un mes y medio después se propuso un acuerdo de [violación](#) de datos de Yahoo! por 117,5 millones de dólares después de que se expusieran más de tres mil millones de cuentas de Yahoo!.



La mejor manera de evitar ser víctima es ser consciente de la amenaza y algunos buenos hábitos de privacidad para prevenir crímenes como los crímenes de identidad de 2019:

- Nunca [haga oprima un enlace ni descargue un archivo adjunto](#) en un correo electrónico o mensaje que no esperaba
- Ignora los mensajes que ofrecen [ofertas increíbles](#) o le amenazan con ir a la cárcel por no cumplir
- Recuerde que las tarjetas de regalo no son de curso legal [para pagar sus impuestos](#) o pagar una tarifa o multa
- Supervise sus cuentas e informe de crédito de forma rutinaria para buscar [cualquier cosa fuera de lo común](#)
- [Congele su informe de crédito](#) si no lo va a usar pronto
- Proteja todas sus cuentas con [contraseñas seguras y singulares](#) que cambie de forma rutinaria



Los consumidores no son responsables de los comportamientos criminales de un pirata cibernético. Sin embargo, puedes tomar medidas que reduzcan el riesgo de ser víctima y ayudar a minimizar el daño si ocurre lo peor. El Centro de Recursos de Robo de Identidad es una organización sin fines de lucro establecida para capacitar y guiar a los consumidores, las víctimas, las empresas y el gobierno para minimizar el riesgo y mitigar el impacto del compromiso de identidad y la delincuencia. Llámalos gratis al 888-400-5530 o visítalos en www.idtheftcenter.org para obtener más información.



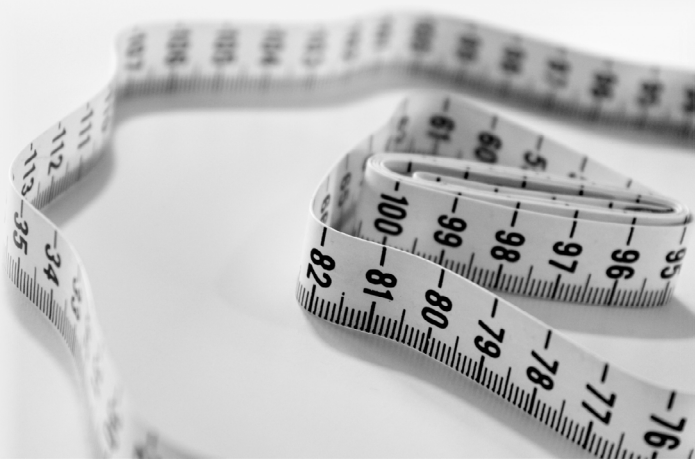
¿Prefieres ahorrar \$5,000 o perder 5 libras?

por Gretchen Abraham, División del Consumidor y Educación Empresarial

Si eligió el dinero, no estará solo. A medida que comenzamos el 2020, muchos de nosotros estamos haciendo resoluciones financieras. Por supuesto, ahorrar más o pagar deudas suena genial, pero empezar puede resultar abrumador. No se preocupe: la FTC tiene cinco ideas para cosas que puede hacer para comenzar bien el nuevo año.

- 1. Haga un presupuesto.** Antes de establecer nuevas metas o hacer cambios, es bueno saber dónde está parado. Use esta [ruta de trabajo para su presupuesto](#) para agregar sus ingresos para el mes pasado y compararlos con cuánto gastó. Tal vez le sorprenda ver a dónde van sus dólares.
- 2. Prioriza tus deudas.** ¿Los pagos de deudas dominan su presupuesto? Haga una lista de sus deudas y sus tasas de interés anuales. Las deudas con las tasas de interés más altas le están costando más: concéntrese en pagarlas primero.
- 3. Empieza pequeño.** Observe su presupuesto para que las áreas reduzcan. Intenta empezar con un pequeño cambio, como invitar a amigos en lugar de salir. Ponga ese dinero a trabajar de inmediato mediante la configuración de transferencias automáticas con su banco o empleador, para que el dinero vaya directamente a su cuenta de ahorros.
- 4. Regístrese para recibir alertas.** Muchos bancos, acreedores y compañías de servicios públicos ofrecen alertas y recordatorios gratuitos cuando sus saldos son bajos o los pagos están por llegar. Estos servicios pueden ayudarlo a evitar cargos por mora, cargos por sobregiro u otros costos inesperados.
- 5. Pida ayuda.** Si tiene una emergencia financiera, no espere hasta que ya haya perdido los pagos. Llame a sus acreedores antes de la fecha de vencimiento, explique la situación y pregunte sobre sus opciones. Muchas empresas trabajarán con usted para crear un plan de pago.

¿Necesita más consejos financieros? No pierda de vista la próxima serie de blogs de la FTC sobre el crédito. Consígalo directamente en su buzón electrónico en ftc.gov/subscribe.



La Comisión Federal de Comercio Reporta Los Principales Fraudes de 2019

Cada año, la Comisión Federal de Comercio (FTC) examina cuidadosamente el número de informes que las personas hacen a la Red Centinela de Consumidores (Consumer Sentinel Network). Durante 2019, la FTC recibió más de 3,2 millones de informes de consumidores. Esto es lo que encontraron cuando examinaron esos informes.

- **Las estafas de impostor fueron el fraude número uno reportado a Centinela en 2019.** Las personas reportaron haber perdido más de \$667 millones por impostores, que a menudo fingían llamar del gobierno o de un negocio conocido, un interés romántico o un miembro de la familia con una emergencia. Cuando las personas perdieron más dinero, fue cuando pagaron a los estafadores con [tarjeta de regalo](#).
- **Impostores del Seguro Social fueron la estafa de impostor del gobierno más alto reportado.** Hubo 166,190 informes sobre la [estafa del Seguro Social](#), y el promedio de pérdida individual fue de \$1,500.
- **Las llamadas telefónicas fueron la forma número uno en que las personas reportaron haber sido contactadas por estafadores.** Mientras que la mayoría de la gente dijo que colgaron esas se who lost money reported a median loss of \$1,000 in 2019.



Los informes de fraude presentados por los consumidores permiten a la FTC y a sus socios encargados de hacer cumplir la ley investigar a las personas y empresas que engañan a las personas para que paguen dinero. Estos informes ayudan a construir y presentar casos contra los estafadores, que también ayuda a hacer cumplir las leyes que detienen las estafas y otras prácticas comerciales deshonestas que toman el dinero de las personas.

De hecho, durante 2019, las acciones policiales de la FTC llevaron a más de \$232 millones en reembolsos a las personas que perdieron dinero. Más de 1,9 millones de personas cobraron cheques enviados por correo por la FTC. Y, en los últimos cuatro años, la gente ha cobrado más de mil millones de dólares en cheques de reembolso de la FTC. Es dinero de verdad en los bolsillos de la gente.

Así que, si usted ha visto una estafa, seguir contándonos sobre ello en [ftc.gov/complaint](https://www.ftc.gov/complaint). Si necesita más información sobre estos principales fraudes, visite [ftc.gov/imposters](https://www.ftc.gov/imposters) y [ftc.gov/giftcards](https://www.ftc.gov/giftcards).



Primero de su clase

Acción de ejecución por parte del Departamento de Justicia



El 28 de enero de 2020, el Departamento de Justicia anunció que había presentado acciones civiles para órdenes de restricción temporal en dos casos históricos contra cinco empresas y tres personas presuntamente responsables de transportar cientos de millones de llamadas robóticas a los consumidores estadounidenses. El Departamento de Justicia alega que se advirtió a las empresas en numerosas ocasiones que estaban llevando a cabo llamadas robóticas fraudulentas —incluidas llamadas gubernamentales y de impostor empresariales— y, sin embargo, continuaron llevando esas llamadas y facilitando los planes de fraude basados en el extranjero apuntando a los estadounidenses. Los llamamientos, la mayoría de los cuales se originaron en la India, dieron lugar a pérdidas financieras masivas para las víctimas de ancianos y vulnerables en todo el país.

Los dos casos contienen alegaciones similares. Los demandados en un caso son Ecommerce National LLC d/b/a TollFreeDeals.com; SIP Retail d/b/a sipretail.com; y su propietario/operadores, Nicholas Palumbo, de 38 años, y Natasha Palumbo, de 33 años, de Scottsdale, Arizona. Los acusados en el otro caso incluyen Global Voicecom Inc., Global Telecommunication Services Inc., KAT Telecom Inc., también conocido como IP Dish, y su propietario/operador, Jon Kahen, de 45 años, de Great Neck, Nueva York. En cada caso, el Departamento de Justicia solicitó una orden que detuviera inmediatamente la transmisión de tráfico ilícito de llamadas robóticas por parte de los acusados. Un tribunal federal ha entrado en una orden de restricción temporal contra los acusados de Global Voicecom.



Los estadounidenses han experimentado un diluvio de llamadas robóticas en los últimos años. Muchas de las llamadas robóticas se originan en el extranjero. Recientemente, los estafadores extranjeros han utilizado llamadas robóticas para hacerse pasar por investigadores del gobierno y para proporcionar a los estadounidenses mensajes alarmantes, tales como: el número de seguro social del destinatario u otra información personal se ha visto comprometida o de otra manera relacionadas con la actividad delictiva; el destinatario se enfrenta a un arresto inminente; sus activos están siendo congelados; sus cuentas bancarias y de crédito tienen actividad sospechosa; sus beneficios están siendo detenidos; se enfrentan a una deportación inminente; o combinaciones de estas amenazas. Cada una de estas afirmaciones es una mentira, diseñada para asustar al destinatario de la llamada en el pago de grandes sumas de dinero. Los impostores del Seguro Social, los impostores del IRS y los esquemas de soporte técnico (en los que las personas que llaman se hacen pasar por empresas de tecnología legítimas) han proliferado en parte debido a la facilidad con la que llamadas robóticas pueden llegar a millones de víctimas potenciales cada hora.

En estos casos, los Estados Unidos alegan que los demandados operaban a los operadores de protocolo de voz sobre Internet (VoIP), que utilizan una conexión a Internet en lugar de líneas telefónicas de cobre tradicionales para llevar llamadas telefónicas. Se alega que numerosas organizaciones criminales con sede en el extranjero utilizaron los servicios de transporte VoIP de los acusados para transmitir llamadas robóticas fraudulentas de fraude de gobierno e impostor empresarial a las víctimas estadounidenses. Las denuncias presentadas en los casos alegan específicamente que los demandados se desempeñaron como “portadores de pasarela”, convirtiéndolos en el punto de entrada de las llamadas iniciadas en el extranjero en el sistema de telecomunicaciones de los Estados Unidos. Los acusados llevaban un número astronómico de llamadas robóticas.

Por ejemplo, la denuncia contra los propietarios/operadores de Ecommerce National d/b/a TollFreeDeals.com alega que los demandados realizaron 720 millones de llamadas durante un período de 23 días de muestra, y que más de 425 millones de esas llamadas duraron menos de un segundo, lo que indica que eran llamadas robóticas. La queja alega además que muchos de los 720 millones de llamadas fueron fraudulentas y utilizaron números de identificación de llamadas falsificados (es decir, falsos). Las llamadas facilitadas por los acusados amenazaron falsamente a las víctimas con una variedad de acciones catastróficas del gobierno, incluyendo la terminación de las prestaciones de seguridad social, la detención inminente por presunto fraude fiscal y la deportación por supuesta falta de llenar los formularios de inmigración correctamente.



Según las denuncias formuladas en ambas denuncias, los acusados ignoraron las banderas rojas repetidas y las advertencias sobre el carácter fraudulento e ilegal de las llamadas que llevaban. Las afirmaciones formuladas en la queja son meras acusaciones de que, si el caso fuera a proceder a juicio, el gobierno debe demostrar recibir una determinación de responsabilidad.

El Departamento de Justicia proporciona una variedad de recursos relacionados con la victimización del fraude de ancianos a través de su Oficina de Víctimas del Delito, a la que se puede llegar a <https://www.ovc.gov>.



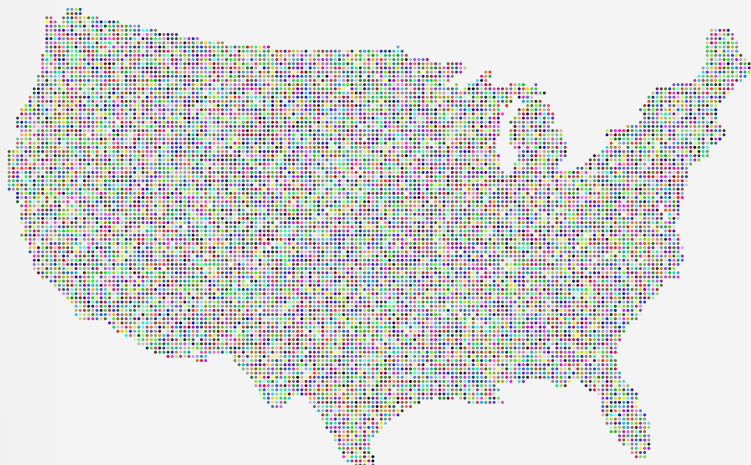
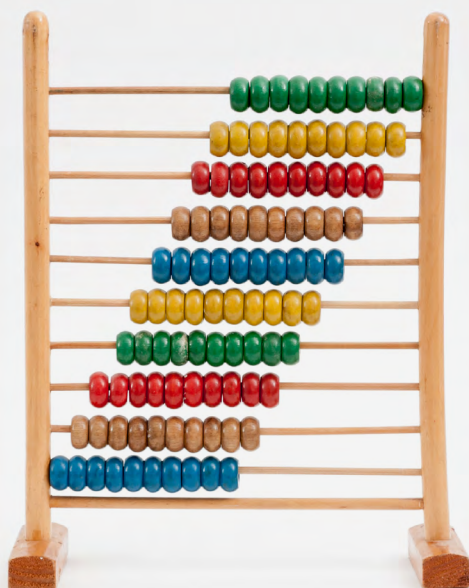
Niños a Menudo Subcontados en el Censo

Aproximadamente una de cada tres resoluciones de Año Nuevo se rompe antes de finales de enero. Este año, hay una resolución que cada familia, comunidad, defensor y líder en Florida debe mantener: asegurándose de que todos los niños sean contados en el Censo 2020.

Más de dos millones de niños se perdieron en el Censo de 2010, más de 71.000 solo en Florida. Este bajo recuento golpeó duramente a las familias de Florida: más de \$67 millones en fondos se perdieron CADA año para el Programa de Cuidado de Crianza, Adopción, Cuidado Infantil y Seguro Médico para Niños.

Pero el subcuento también dañó los fondos para nuestras escuelas, carreteras, Medicare, Medicaid, preparación para emergencias (es decir, huracanes) y mucho más. Dado que el Censo ocurre sólo una vez cada 10 años, estas pérdidas de financiamiento perjudican a los niños durante la mayor parte de su infancia.

Para obtener más información, visite [Más información: Asegurémonos de que todos los niños se cuenten.](#)



EN MARZO

**SEMANA NACIONAL DE
PROTECCION AL CONSUMIDOR:
1-7 DE MARZO, 2020**

**SEMANA NACIONAL DE
TOPOGRAFOS:
15-21 DE MARZO, 2020**



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 creen que se ha producido un fraude pueden ponerse en contacto con la línea directa de información y protección del consumidor del departamento llamando al 1-800-HELP-FLA (435-7352) o, para los hispanohablantes, al 1-800-FL-AYUDA (352-9832) o visítenos en línea en FloridaConsumerHelp.com.

Síguenos en Twitter- @FDACS y @NikkiFriedFL

FDACS-P-02160 Rev. 02/2020