Esta guía explica, cómo prevenir el robo de identidad, reconocer señales de alerta y actuar rápidamente si sospecha que alguien está usando su información personal.

Robo de identidad:
El robo de identidad ocurre cuando alguien usa su información personal o financiera sin su permiso. La prevención empieza con proteger sus datos, revisar sus cuentas y actuar ante señales inusuales.

Proteja	Revise	Verifique	Reporte
Guarde y destruya documentos con datos personales.	Verifique cuentas, facturas e informes de crédito.	No comparta datos por llamadas, emails o textos inesperados.	Use RobodeIdentidad.gov si sospecha robo de identidad.

1. ¿Qué es el robo de identidad?

El robo de identidad ocurre cuando una persona usa su información personal o financiera sin su autorización para obtener dinero, servicios, crédito o beneficios a su nombre.

- Su nombre, dirección, fecha de nacimiento o número de teléfono.
- Números de tarjetas de crédito, cuentas bancarias o credenciales en línea.
- Número de Seguro Social o información de seguro médico.
- Información que aparece en facturas, estados de cuenta, correo o formularios.

¿Para qué pueden usar sus datos?

Comprar con sus tarjetas

Cargos que usted no reconoce.

Abrir cuentas nuevas

Tarjetas, préstamos o servicios bajo su nombre.

Cambiar su dirección

Para desviar facturas o correspondencia.

Robar reembolsos o beneficios

Impuestos, beneficios o pagos que le correspondan.

Obtener servicios médicos

Uso indebido de información médica.

Hacerse pasar por usted

Incluyendo trámites, solicitudes o situaciones legales.

Recuerde

No es necesario que le roben todos sus datos para causar daño. A veces basta con una combinación de nombre, número de Seguro Social, fecha de nacimiento, número de cuenta o contraseña.

2. Señales de alerta: ¿cómo saber si alguien usa su identidad?

Mientras más rápido detecte un problema, más rápido podrá limitar el daño. Revise estas señales con frecuencia:

Deja de recibir una factura o estado de cuenta

Puede indicar que alguien cambió su dirección.

Aparecen cargos que usted no hizo

Revise tarjetas de crédito, débito y cuentas digitales.

Hay retiros o transferencias desconocidas

Comuníquese con su institución financiera de inmediato.

Recibe una factura inesperada

Podría ser una cuenta abierta o servicio activado a su nombre.

Su informe de crédito muestra cuentas que no reconoce

Solicite y revise sus informes de crédito.

Lo contactan por una deuda que no es suya

No ignore la comunicación; pida información por escrito.

Recomendación:
Una vez por semana revise sus cuentas bancarias y tarjetas. Una vez al mes revise facturas y estados de cuenta. Periódicamente revise sus informes de crédito gratuitos.

3. Prevención práctica: pasos que puede comenzar hoy

Use esta lista como guía de hábitos de protección. No tiene que hacerlo todo en un día: comience con los pasos de mayor riesgo para usted.

A. Proteja documentos físicos

- Guarde en un lugar seguro tarjetas de Seguro Social, Medicare, estados de cuenta y documentos con datos personales.
- Antes de botar documentos, tritúrelos o tache números de cuenta con marcador permanente.
- Recoja su correspondencia lo antes posible y evite dejar documentos visibles en vehículos u oficinas.

B. Cuide su número de Seguro Social

- No lo comparta por teléfono, email o mensaje de texto cuando alguien lo contacte inesperadamente.
- Antes de darlo, pregunte: ¿para qué lo necesitan?, ¿cómo lo protegerán?, ¿puedo usar otro documento?, ¿bastan los últimos cuatro dígitos?
- Si las respuestas no le convencen, no lo comparta.

C. Fortalezca sus cuentas digitales

- Use contraseñas largas, únicas y difíciles de adivinar.
- Active autenticación de dos factores o *multifactor* cuando esté disponible.
- No abra enlaces ni archivos de mensajes sospechosos; entre directamente a la página oficial.

D. Proteja su crédito

- Considere un congelamiento de crédito si no está solicitando crédito nuevo.
- Use una alerta de fraude si sospecha que alguien intenta abrir cuentas a su nombre.
- Revise sus informes de crédito para detectar cuentas que no reconoce.

E. Verifique antes de confiar

- Desconfíe de presión, urgencia, amenazas o promesas demasiado buenas para ser ciertas.
- Confirme la identidad de quien llama usando un número oficial, no el número que aparece en el mensaje.
- Antes de entrar datos, confirme que la página sea oficial y segura.

F. Haga seguimiento

- Revise cuentas, facturas y notificaciones de instituciones financieras.
- Active alertas de transacciones si su banco o tarjeta las ofrece.
- Guarde evidencia de comunicaciones sospechosas.

4. Dos herramientas importantes: congelamiento de crédito y alerta de fraude

Estas herramientas pueden ayudar a que sea más difícil abrir cuentas nuevas a su nombre. Funcionan de manera diferente y pueden usarse según su situación.

Herramienta	¿Qué hace?	¿Cuándo considerarla?
Congelamiento de crédito	Impide que se acceda a su informe de crédito para abrir cuentas nuevas mientras esté activo. Se puede levantar cuando necesite solicitar crédito.	Cuando desea mayor protección o no está solicitando crédito nuevo.
Alerta de fraude	Indica a los negocios que deben verificar su identidad antes de abrir una cuenta nueva a su nombre. Una alerta inicial dura un año.	Cuando sospecha fraude, pérdida de datos o posible uso indebido de su información.
Informes de crédito	Le permiten revisar cuentas, consultas y datos que aparecen bajo su nombre.	Para detectar cuentas que no reconoce, errores o actividad sospechosa.

¿Cómo lo hago?

Para congelar su crédito, normalmente debe comunicarse con cada una de las tres compañías principales de informes de crédito: *Equifax, Experian y TransUnion*. Para una alerta de fraude inicial, puede comunicarse con una de ellas y esa compañía debe notificar a las otras.

*Antes de pagar por monitoreo de identidad

Los servicios de monitoreo pueden avisarle sobre ciertos cambios, pero no detectan todo. Por ejemplo, no siempre alertan sobre retiros de una cuenta bancaria, uso indebido del Seguro Social para impuestos o algunos beneficios. Antes de pagar, pregunte qué monitorean, con qué frecuencia, cuánto cuesta y qué no cubren.

5. ¿Qué hacer si sospecha robo de identidad?

Actúe rápido. Mantenga la calma, documente lo ocurrido y siga un orden para evitar más daño.

1. Detenga el riesgo inmediato: Cambie contraseñas, active autenticación *multifactor* y cierre sesiones desconocidas.

2. Avise a su banco o emisor de tarjeta: Reporte cargos, retiros o transacciones no autorizadas y solicite bloqueo o reemplazo de tarjetas si aplica.

3. Revise sus informes de crédito: Busque cuentas nuevas, consultas o direcciones que no reconoce.

4. Coloque una alerta de fraude o congelamiento: Use la herramienta que mejor responda a su situación.

5. Reporte el robo de identidad: Visite RobodeIdentidad.gov para recibir un plan de acción gratuito y personalizado.

6. Guarde evidencia: Conserve capturas, cartas, números de reclamación, fechas, nombres y copias de todo lo enviado o recibido.

Recurso oficial:

Si cree que alguien le robó su identidad, la FTC recomienda reportarlo en RobodeIdentidad.gov. El sitio ofrece un plan de acción, seguimiento de avances y cartas o formularios precompletados para comunicarse con compañías e instituciones.

6. *Checklist* rápido de prevención

Marque las acciones que ya realiza y seleccione una o dos para comenzar esta semana.

Acción	Sí	Pendiente
Reviso mis cuentas bancarias y tarjetas regularmente.	☐	☐
Tengo alertas activas de transacciones o compras, si mi institución las ofrece.	☐	☐
Uso contraseñas distintas para mis cuentas importantes.	☐	☐
Tengo autenticación de dos factores o multifactor activada.	☐	☐
No comparto mi Seguro Social por llamadas, emails o textos inesperados.	☐	☐
Trituro o tacho documentos con información personal antes de botarlos.	☐	☐
Recojo mi correspondencia rápidamente.	☐	☐
Reviso mis informes de crédito gratuitos.	☐	☐
Sé cómo comunicarme con mi banco o cooperativa si veo una transacción sospechosa.	☐	☐
Sé que puedo reportar robo de identidad en RobodeIdentidad.gov.	☐	☐

7. Recursos oficiales y recordatorios finales

RobodeIdentidad.gov Reporte robo de identidad y reciba un plan de acción personal y gratuito. www.robodeidentidad.gov	**IdentityTheft.gov** Versión en inglés para reportar robo de identidad. www.identitytheft.gov
AnnualCreditReport.com Sitio autorizado para solicitar informes de crédito gratuitos. www.annualcreditreport.com	**Consumer.FTC.gov** Consejos para consumidores sobre seguridad, fraude y robo de identidad. consumidor.ftc.gov

Mensaje final

La mejor defensa es la vigilancia constante: proteja sus documentos, cuestione solicitudes inesperadas, revise sus cuentas y actúe rápido ante cualquier señal sospechosa.

*Fuente principal

Comisión Federal de Comercio (FTC), Consumer Advice: "Lo que hay que saber sobre el robo de identidad"; FTC: "Credit Freezes and Fraud Alerts"; AnnualCreditReport.com. Esta guía resume información educativa y no sustituye asesoramiento legal o financiero individual.