



# Robo de identidad

## Qué saber.



### ¿Qué es?

Identity theft is when someone gets your personal information and uses it to commit fraud.

Pretending to be you, they could:

- cometer otros delitos;
- abrir nuevas tarjetas de crédito en tu nombre;
- robar dinero de tus cuentas;
- alquilar apartamentos;
- solicitar préstamos.

Estamos aquí para ayudarte:

Para tarjetas de crédito, llama al **1-800-955-9060**

Para banca personal, llama al **1-800-935-9935**

Para financiación de vehículos, llama al **1-800-336-6675**

Para préstamos para vivienda, llama al **1-800-848-9136**

Para más detalles, visita: [chase.com/SecurityCenter](http://chase.com/SecurityCenter)



### Qué buscar

- Transacciones inexplicables con tarjetas de crédito o cuentas bancarias.
- Nuevas tarjetas de crédito o cuentas financieras que tú no solicitaste.
- Rechazo inesperado de una solicitud de crédito.
- No recibes correos o emails que estás esperando.
- Consultas desconocidas sobre tu informe de crédito, llamadas de cobradores de deudas o una solicitud rechazada que no enviaste.
- Una caída sorpresa en tu puntaje de crédito.
- Actividad inusual en tu cuenta del Seguro Social.



### Cómo sucede

#### Phishing (pronunciado "pesca") o smishing

Esto sucede cuando los estafadores envían emails o mensajes de texto que parecen ser de un sitio conocido e intentan engañarte para que proporciones información personal o introducen malware en tu dispositivo.

#### Hacking

Esto es cuando un ladrón obtiene acceso a tu información usando tecnología para entrar en tu computadora, dispositivo o red.

#### Suplantación de identidad

Estos son sitios web o números de teléfono falsos que parecen legítimos y te piden que proporciones información personal.

#### Robo

Un ladrón te roba el correo postal, documentos personales, estados de cuenta financieros, la computadora portátil, el teléfono inteligente u otro dispositivo.



### Cómo ayudar a minimizar riesgos

- Ten cuidado con tus documentos, dispositivos y propiedades.
- No proporciones nunca tu información personal a nadie que te llame por teléfono, te envíe mensajes de texto o te mande emails.
- Como mínimo, ten contraseñas únicas para tus cuentas financieras y no uses las mismas en distintos sitios.
- Verifica a menudo tus informes de crédito para monitorear cualquier cambio inesperado.
- Accede a tu puntaje de crédito gratuito y al monitoreo de identidad con Chase Credit Journey®. Recibe alertas si hay cambios en tu informe de crédito o si tu información aparece en la web oscura, usando [chase.com/CreditJourney](http://chase.com/CreditJourney).
- Considera comunicarte con las 3 agencias de informes de crédito para acceder a herramientas para proteger tu informe de crédito o puntaje de crédito.
- No hagas clic nunca en enlaces o archivos adjuntos en emails sospechosos; si no sabes si es legítimo, ve directamente al sitio web de la organización.
- Lleva contigo solo las cosas que necesites (y evita llevar tu tarjeta del Seguro Social) en caso de pérdida o robo.



# Robo de identidad

Qué hacer si crees que has sido víctima de robo de identidad:

Estamos aquí para ayudarte:

Para tarjetas de crédito, llama al **1-800-955-9060**

Para banca personal, llama al **1-800-935-9935**

Para financiación de vehículos, llama al **1-800-336-6675**

Para préstamos para vivienda, llama al **1-800-848-9136**

Para más detalles, visita: [chase.com/SecurityCenter](https://chase.com/SecurityCenter)



## Notifica a las compañías o bancos pertinentes

- Comunícate con las compañías y bancos pertinentes de inmediato para alertarlos sobre el problema.
- Reporta la actividad que crees que haya sido fraudulenta con ellos.



## Comunícate con las 3 agencias de informes de crédito para revisar tu actividad

- Obtén informes de crédito de las 3 agencias para buscar instancias de fraude. Si sospechas que ha habido fraude, notifica a las 3 agencias de informes de crédito para investigar y resolver la actividad. Considera agregar una alerta de congelamiento o fraude. Una alerta de fraude notificará a otros que es posible que hayas sido víctima de fraude, mientras que un congelamiento impide el uso de tu crédito sin tu aprobación.

### Equifax:

800-525-6285 | [equifax.com](https://equifax.com)

### Experian:

888-397-3742 | [experian.com](https://experian.com)

### TransUnion:

888-909-8872 | [transunion.com](https://transunion.com)



## Comunícate con las fuerzas del orden público locales

- Proporciona toda la información que puedas, incluyendo fechas, horas y números de cuenta exactos.
- Presenta una denuncia policial si alguien lo recomienda.
- Guarda una copia de la denuncia policial ya que algunos negocios o instituciones financieras podrían pedírtela para retirar cualquier cargo fraudulento.



## Reporta cualquier robo de identidad a la Comisión Federal de Comercio

- La FTC se dedica a proteger a los consumidores de EE. UU.
- Ve a su sitio web, [identitytheft.gov](https://identitytheft.gov), para presentar un informe y obtener un plan de recuperación.
- Cuando presentes un informe, la FTC y otras agencias podrán usar tu información para iniciar casos contra estafadores.



## Refuerza tu seguridad

- Cambia los nombres de usuario y contraseñas en todas tus cuentas activas. Usa contraseñas únicas para tus cuentas financieras y no uses las mismas en distintos sitios. Considera usar un administrador de contraseñas para crear y almacenar contraseñas seguras.
- Mantén tu teléfono, computadora y navegadores web actualizados, ya que a menudo hay parches de seguridad incluidos con las actualizaciones del sistema.
- En los sitios que lo ofrezcan, usa la autenticación multifactor, ya que requiere más que solo una contraseña para iniciar sesión.

