Robo de identidad

Estamos a su disposición para ayudar:

Para tarjetas de crédito, llame al **1-800-955-9060**
Para banca personal, llame al **1-800-935-9935**
Para financiación de vehículos, llame al **1-800-336-6675**
Para préstamos para vivienda, llame al **1-800-848-9136**

Para más detalles, visite: **chase.com/securitycenter**

Qué debe saber.

¿Qué es?

El robo de identidad es cuando alguien obtiene su información personal y la utiliza para cometer fraude.

Haciéndose pasar por usted, podrían:

- Cometer otros delitos
- Abrir nuevas tarjetas de crédito a su nombre
- Robar dinero de sus cuentas
- Alquilar apartamentos
- Solicitar préstamos

Qué buscar.

- Transacciones inexplicables en tarjetas de crédito o cuentas bancarias
- Nuevas tarjetas de crédito o cuentas financieras que no haya solicitado
- Denegación inesperada de una solicitud de crédito
- No se recibe correo postal ni correos electrónicos esperados
- Consultas desconocidas en su informe de crédito, llamadas de cobradores de deudas o rechazo de una solicitud que no presentó
- Una caída sorpresa en el puntaje de crédito
- Actividad inusual en su cuenta del Seguro Social

Cómo sucede.

Suplantación de identidad (phishing) (pronunciado “fishing”) o **Robo de identidad por mensaje de texto (SMiShing)**

Esto es cuando los estafadores envían correos electrónicos o mensajes de texto que parecen de buena reputación tratando de engañarle para que proporcione información personal o infectarle su dispositivo con software malicioso.

Piratería (hacking)

Esto es cuando un ladrón obtiene acceso a su información personal utilizando tecnología para irrumpir en su computadora, dispositivos o red.

Suplantación de identidad (spoofing)

Estos son sitios web o números telefónicos falsos que se ven legítimos y le piden proporcionar información personal.

Robo

Un ladrón se apropia de su correo postal, documentos personales, estados financieros, computadora portátil, teléfono inteligente u otro dispositivo.

Cómo ayudar a minimizar el riesgo.

- Esté atento a sus documentos, dispositivos y propiedad.
- Nunca proporcione su información personal a alguien que le llame, envíe mensajes de texto o correos electrónicos.
- Como mínimo, tenga contraseñas únicas para sus cuentas financieras y no las utilice en todos los múltiples sitios web.
- Revise periódicamente su informe de crédito para supervisar cambios que no anticipó.
- Regístrese para la supervisión gratuita del puntaje de crédito e identidad con Chase Credit Journey® y reciba alertas por cambios en su informe de crédito o si su información se encuentra en la red oscura (dark web) en **chase.com/creditjourney**
- Considere comunicarse con las tres agencias de informes de crédito para obtener herramientas para proteger su informe de crédito o puntaje de crédito.
- Nunca haga clic en ningún enlace o archivos adjuntos en correos electrónicos sospechosos. Si no está seguro de que sea legítimo, visite directamente el sitio web de la organización.
- Lleve consigo solo lo que necesita (y nunca su tarjeta de Seguro Social), en caso de pérdida o robo.

Robo de identidad

Estamos a su disposición para ayudar:

Para tarjetas de crédito, llame al **1-800-955-9060**
Para banca personal, llame al **1-800-935-9935**
Para financiación de vehículos, llame al **1-800-336-6675**
Para préstamos para vivienda, llame al **1-800-848-9136**

Para más detalles, visite: **chase.com/securitycenter**

Qué hacer si cree que le han robado su identidad.

Notifique a las compañías o bancos relevantes

- ☐ Comuníquese con las compañías o bancos relevantes de inmediato para alertarlos del problema.
- ☐ Dispute con ellos la actividad que cree que es fraudulenta.

Comuníquese con las tres agencias de informes de crédito para revisar la actividad

- ☐ Obtenga los informes de crédito de las tres agencias para buscar si ha habido fraude. Si sospecha que hubo fraude, notifique a las tres agencias de informes de crédito para investigar y resolver la actividad. Considere agregar un bloqueo o alerta de fraude. Una alerta de fraude notificará a otros que usted podría ser víctima de fraude, mientras que un bloqueo impide el uso de su crédito sin su aprobación.

Equifax:
800-525-6285 | **equifax.com**

Experian:
888-397-3742 | **experian.com**

TransUnion:
888-909-8872 | **transunion.com**

Comuníquese con la agencia del orden público local

- ☐ Provea toda la información que pueda, incluyendo fechas, horas y números de cuenta exactos.
- ☐ Presente una denuncia policial si se recomienda.
- ☐ Guarde una copia de la denuncia policial porque algunas compañías o instituciones financieras pueden requerirlo para eliminar cualquier cargo fraudulento.

Informe su robo de identidad a la Comisión Federal de Comercio

- ☐ La Comisión Federal de Comercio (FTC) se dedica a proteger a los consumidores en Estados Unidos / EE. UU.
- ☐ Visite su sitio web, **identitytheft.gov**, para presentar un informe y obtener un plan de recuperación.
- ☐ Cuando presenta un informe, la FTC y otras agencias utilizan su información para establecer casos contra los estafadores.

Refuerce su seguridad

- ☐ Cambie los nombres de usuario y contraseñas de todas sus cuentas activas. Tenga contraseñas únicas para sus cuentas financieras y no las repita en distintos sitios web. Considere utilizar un administrador de contraseñas para crear y almacenar contraseñas seguras.
- ☐ Mantenga actualizados su teléfono, computadora y navegadores web, ya que a menudo se incluyen parches de seguridad con las actualizaciones del sistema.
- ☐ Utilice la autenticación multifactor en los sitios web que la ofrecen, ya que requiere más que una simple contraseña para iniciar sesión.