



ROBO DE IDENTIDAD

En una era caracterizada por la interconexión digital, el riesgo de robo de identidad se ha incrementado. Las actividades en línea, como socializar y hacer compras, ofrecen tanto comodidad como posibles peligros. A medida que la tecnología evoluciona, también lo hacen las tácticas de los delincuentes informáticos que buscan hacer un uso indebido de los datos personales de otras personas para su beneficio. Es fundamental comprender las amenazas y aprender estrategias proactivas para proteger su identidad.

CONSEJOS RÁPIDOS

- Guarde los documentos confidenciales en un armario cerrado con llave o use un sistema de almacenamiento digital seguro. Evite llevar consigo documentos de identificación innecesarios y destruya los estados financieros antiguos antes de deshacerse de ellos.
- Cree contraseñas únicas y seguras para todas las cuentas en línea y evite usar información fácil de adivinar, como cumpleaños o nombres. Habilite la autenticación multifactor siempre que sea posible.
- Proporcione información personal solo en sitios web seguros con "https://" en la dirección URL. Desconfíe de los correos electrónicos o las llamadas no solicitados en los que se le pidan datos confidenciales, y nunca comparta datos personales por teléfono a menos que usted haya iniciado la llamada.
- Revise periódicamente los estados de cuenta bancarios y de tarjetas de crédito para detectar transacciones no autorizadas. Suscríbase a alertas de cuenta para recibir notificaciones de actividades sospechosas.
- Considere la posibilidad de congelar su crédito para evitar el acceso no autorizado a su información financiera. Esto brinda una capa adicional de protección y evita que los estafadores abran nuevas cuentas a su nombre.

CONSEJOS DE SEGURIDAD SOBRE ROBO DE IDENTIDAD

PREVENCIÓN

- Si recibe correo con su información personal, asegúrese de retirarlo de su bandeja de entrada lo antes posible cada día.
- Tenga cuidado con los correos electrónicos, mensajes de texto o enlaces sospechosos. Los delincuentes informáticos a menudo intentan engañarle para que comparta información personal. Verifique siempre la fuente antes de hacer clic.
- Proteja su número de seguro social. No lleve consigo su tarjeta del seguro social y evite compartir el número a menos que sea necesario. Pregunte a la organización que se lo solicita el motivo, cómo protegerá el número y si puede proporcionar solo los últimos cuatro dígitos o información de identificación diferente.
- Use contraseñas complejas con una combinación de letras, números y símbolos. Evite usar información fácil de adivinar, como cumpleaños o nombres.
- Use un software antivirus confiable y mantenga sus dispositivos actualizados con los últimos parches de seguridad.
- Evite usar Wi-Fi pública para transacciones confidenciales y opte por una red privada virtual (VPN) cuando acceda a Internet sobre la marcha.
- Use una contraseña segura para proteger la red Wi-Fi de su hogar.
- Ajuste la configuración de privacidad en las plataformas de redes sociales para limitar quién puede ver su información personal y sus publicaciones.
- Los ladrones de identidad pueden hacerse pasar por agencias gubernamentales, instituciones financieras o incluso conocidos. Antes de compartir información, verifique siempre la autenticidad de las solicitudes de información personal.
- Siempre que sea posible, habilite la autenticación multifactor para sus cuentas en línea. Esto brinda una capa adicional de seguridad al requerir un segundo paso de verificación.

DETECCIÓN

Las siguientes son algunas formas en las que puede descubrir si se ha producido un robo de identidad:

- Las organizaciones pueden notificarle si sus datos se han visto afectados por una filtración de datos.
- Si le dejan de llegar las facturas que tiene pendientes, puede ser señal de que alguien ha alterado su dirección de facturación. Del mismo modo, empezar a recibir facturas por servicios que no utiliza también podría ser una señal de que alguien está utilizando su identidad para abrir nuevas cuentas.
- Compruebe sus estados de cuenta bancarios y financieros, incluidos los del seguro social, para detectar errores o cargos que no haya autorizado.
- Obtenga informes de crédito gratuitos de las tres agencias principales anualmente y reviselos para detectar discrepancias o actividades sospechosas. Informe de inmediato sobre cualquier discrepancia.
- Es posible que le nieguen inesperadamente un crédito, incluidas las tarjetas de crédito o los préstamos, o que su puntuación de crédito cambie inesperadamente.
- Es posible que le notifiquen que se ha presentado una declaración de impuestos en su nombre sin su conocimiento.

INFORMES

Si sospecha que puede ser víctima de un robo de identidad, puede obtener ayuda de organizaciones de confianza.

- Inicie un registro de todas las conversaciones que tenga y los pasos que dé a medida que comience a lidiar con la situación.
- Informe sobre sus sospechas a su banco y a sus instituciones financieras.
- Póngase en contacto con las tres principales agencias de crédito. Pídale que coloquen alertas de fraude y bloqueos de crédito en sus cuentas.
- Póngase en contacto con la Comisión Federal de Comercio y siga los pasos recomendados en www.identitytheft.gov.