

**OUCH!**

El Boletín Mensual de Concientización en Seguridad para ti

Robo de identidad - Cómo protegerte

¿Qué es el robo de identidad?

El robo de identidad sucede cuando un criminal roba información tuya y la utiliza para cometer fraudes, como solicitar beneficios por desempleo, devolución de impuestos, un nuevo préstamo o tarjetas de crédito a tu nombre. Si no tomas precauciones, puedes terminar pagando por productos o servicios que no compraste y lidiando con el estrés y la angustia financiera que sigue al robo de identidad.

Tu información personal existe en numerosos lugares en Internet. Todo el tiempo que navegas o compras algo en línea, ves un video, compras comestibles, visitas a tu médico o utilizas una aplicación en tu smartphone, se recopila información sobre ti. Esa información suele ser frecuentemente vendida o compartida con otras empresas. Incluso si solo una de estas es hackeada, los criminales pueden tener acceso a tu información personal. Asume que algo de información sobre ti se encuentra ya disponible para los criminales y considera lo que puedes hacer para frenar o detectar el uso de tu información para cometer fraudes.

Cómo detectarlo

- Revisa tus tarjetas y otras cuentas con regularidad para detectar cualquier cargo o pago que no hayas realizado. Una forma sencilla de hacer esto es registrarse para recibir notificaciones por correo electrónico, mensajes de texto o de aplicaciones móviles para pagos y otras transacciones. Monitoréalas para detectar fraudes.
- Investiga situaciones en las que los comerciantes rechacen tus tarjetas de crédito o débito. Busca notificaciones o llamadas telefónicas de cobradores de deudas en busca de pagos atrasados de tarjetas de crédito, facturas médicas o préstamos que sepas que no son tuyos.
- Presta atención a las notificaciones del gobierno acerca de beneficios por desempleo u otros que nunca pediste.
- Si está disponible en tu localidad, revisa tus informes de crédito al menos una vez al año. Por ejemplo, en los Estados Unidos, puedes solicitar informes gratuitos en annualcreditreport.com.

Qué hacer cuando suceda

- Comunícate con la organización involucrada en el fraude. Por ejemplo, si un delincuente abrió una tarjeta de crédito a tu nombre, llama a la compañía de la tarjeta de crédito para notificar sobre el fraude. Si alguien solicitó un reembolso de impuestos o beneficios por desempleo a tu nombre, comunícate con la organización gubernamental correspondiente.

- Levanta una denuncia ante las autoridades competentes para crear un registro oficial de robo de identidad. A menudo puedes hacer esto en línea. Por ejemplo, en los Estados Unidos puedes reportar en [identitytheft.gov](https://www.identitytheft.gov). Sigue las instrucciones del sitio para cualquier paso adicional que debas realizar.
- Para responder ante un fraude, guarda los registros de tus interacciones con la institución financiera y las autoridades, así como los costos en los que incurras por robo de identidad, en caso de que estos detalles sean necesarios después.
- Notifica a tu compañía de seguros; es posible que tengas protección ante robo de identidad incluido en tu póliza.

Cómo defenderte ante esto

Aquí te compartimos algunos pasos simples que puedes tomar para reducir la probabilidad de ser víctima de fraude:

- Limita la información que compartes de ti mismo en servicios en línea o sitios web.
- Utiliza una contraseña fuerte y única de todas tus cuentas en línea y habilita el doble factor de autenticación como protección adicional de tus cuentas más importantes.
- Si aplica en tu localidad, restringe quién puede tener acceso a tus reportes de crédito. Por ejemplo, en los EE.UU. Puedes realizar el congelamiento de tu crédito, de esta manera cualquiera que trate de obtener una tarjeta de crédito o préstamo a tu nombre primero tendrá que descongelarlo temporalmente.
- Considera adquirir cobertura de seguro, ya sea a través de una póliza dedicada o como parte de tu plan de seguro existente, que cubra los costos de lidiar con el robo de identidad.

Editor invitado

Lenny Zeltser es el CISO de Axonius, una empresa de gestión de activos de ciberseguridad. También enseña cómo desarrollar y combatir malware en el Instituto SANS. Lenny se encuentra en Twitter como [@lennyzeltser](https://twitter.com/lennyzeltser) y en su blog de seguridad zeltser.com.



Recursos

Ingeniería social: <https://www.sans.org/security-awareness-training/resources/social-engineering-attacks>

Creando contraseñas simples: <https://www.sans.org/security-awareness-training/resources/making-passwords-simple>

Reporta robo de identidad: <https://www.identitytheft.gov>

Congelamiento de crédito: <https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/>

Robo de identidad: <https://zeltser.com/unemployment-fraud-and-identity-theft/>

Traducido para la comunidad por: Cécica Martínez Aponte, UNAM-CERT

OUCH! Es publicado por SANS Security Awareness y distribuido bajo la licencia [Creative Commons BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/). Puedes distribuir y compartir este boletín, siempre y cuando no lo vendas o modifiques. Consejo editorial: Walter Scrivens, Phil Hoffman, Alan Waggoner, Les Ridout, Princess Young