

¿Está segura su identidad? Qué hacer si no es así

Por Mariana Raymond de Truecaller (NAPS)—El robo de identidad se está volviendo más común y afecta a todo tipo de personas, pero usted puede protegerse.

El problema

Los estafadores siempre encuentran nuevas formas de robar información personal, lo que a menudo deja a sus víctimas con pérdidas financieras y una sensación de violación.

Una respuesta

Mantenerse informado hacer una gran diferencia para permanecer seguro. Esto es lo que usted debe saber:

Cómo ocurre el robo de identidad

La mayoría de los robos de identidad ocurren en línea. A menudo, cuando alguien hace clic en enlaces de mensajes de texto, correos electrónicos o es engañado. El enlace en el que hace clic podría llevarlo a un sitio web falso para ingresar credenciales o instalar una aplicación que pueda capturar sus contraseñas de cuentas importantes.

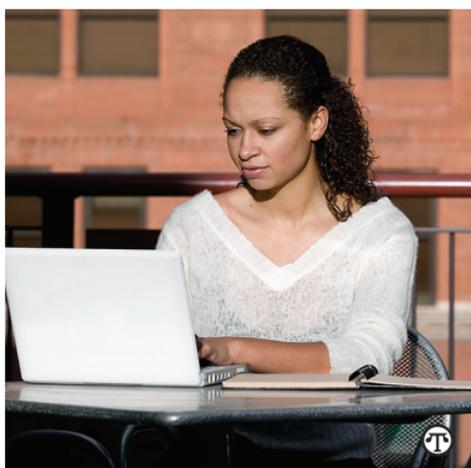
Robo de identidad en aumento

- **Robo de identidad sintético:** Con el robo de identidad sintético, los estafadores mezclan información real y falsa para crear una identidad nueva y falsa. Es posible que utilicen un número de seguro social real junto con detalles inventados. Esto les permite abrir cuentas bancarias, obtener tarjetas de crédito y pedir préstamos, usando una identidad falsa que parece demasiado real.
- **Robo de identidad médica:** el robo de identidad médica ocurre cuando alguien usa su información médica para acceder a servicios de atención médica, medicamentos recetados o dispositivos médicos. Esto puede generarle facturas médicas inesperadas o registros inexactos, lo que puede complicar tratamientos futuros. Es una situación frustrante, pero saber qué buscar puede ayudar.
- **Fraude de apropiación de cuentas:** en el fraude de apropiación de cuentas, los estafadores toman control de sus cuentas en línea, como cuentas bancarias, correo electrónico o redes sociales. Esto suele ocurrir a través de correos electrónicos phishing, contraseñas débiles o violaciones de datos. Una vez dentro, los estafadores pueden drenar sus fondos o robar aún más datos personales. Da miedo, pero hay formas de protegerse.
- **Robo de identidad profundo e impulsado por IA:** a medida que avanza la tecnología, los delincuentes utilizan herramientas como inteligencia artificial (IA) para crear perfiles falsos: vídeos o voces falsos que parecen y suenan como personas reales. Pueden usarlos para engañar a otros haciéndoles creer que son otra persona. Es un problema de alta tecnología, pero no es necesario ser un experto en tecnología para defenderse.

Maneras de protegerse

Ninguna solución es infalible, pero hay 7 pasos que usted puede seguir para protegerse y reducir las posibilidades de convertirse en una víctima:

1. Usar una aplicación de identificación de llamadas y bloqueo de estafadores: la aplicación Truecaller ayuda a identificar llamadas y mensajes desconocidos e identificará números fraudulentos en tiempo real. Personas



El robo de identidad puede ocurrirle a cualquiera, pero usted puede tomar medidas para protegerse.

de todo el mundo denuncian activamente números como estafas y escriben comentarios sobre su experiencia y usted puede ver estadísticas sobre los patrones de llamadas de los estafadores.

2. Utilice contraseñas seguras y únicas: cree contraseñas difíciles de descifrar: combine letras, números y símbolos. Evite reutilizar contraseñas. Un administrador de contraseñas puede ser una herramienta útil para crear y guardar contraseñas de forma segura.

3. Habilite Multi-Factor Authentication: MFA agrega una capa adicional de seguridad a sus cuentas. Después de ingresar su contraseña, deberá verificar su identidad nuevamente, como con un código enviado a su teléfono. Es como agregar una segunda cerradura a su puerta, lo que dificulta que los estafadores entren por la fuerza.

4. Controle su crédito con regularidad: Esté atento a sus informes de crédito para detectar cualquier cosa inusual, como cuentas nuevas que no abrió. Es una de las formas más rápidas de detectar el robo de identidad a tiempo. Muchos lugares ofrecen servicios gratuitos de monitoreo de crédito. Aprovéchelos.

5. Considere servicios de protección contra el robo de identidad: algunos servicios pueden controlar su información personal y alertarlo si detectan algo sospechoso. Si bien no pueden prevenir el robo de identidad, pueden facilitar el proceso de recuperación si le sucede a usted.

6. Proteja sus dispositivos: mantenga su teléfono, computadora y otros dispositivos actualizados con los últimos parches de seguridad. Utilice software antivirus y contraseñas seguras para mantener alejados a los piratas informáticos. Es un hábito simple que puede ser de gran ayuda.

7. Destruya documentos importantes: Incluso en la era digital actual, el papeleo físico puede seguir siendo una mina de oro para los ladrones. Triture todos los documentos que contengan información personal (extractos bancarios o facturas médicas) antes de tirarlos.

Mantenerse informado sobre las últimas estafas y tener cuidado con su información puede marcar una gran diferencia. Y si se convierte en víctima, no entre en pánico. Repórtelo a las autoridades o a su buró de crédito de inmediato. Pueden ayudarlo a limitar el daño e iniciar el proceso de recuperación.

Aprenda más

Para obtener más datos y consejos, visite www.truecaller.com.