Robo de identidad y fraude: cómo evaluar y gestionar los riesgos

Escrito por Adraemond - 22/01/2024 21:44

---

verificacion de identidad para originacion

El fraude y el robo de identidad se han extendido a lo largo de los años, dejando a su paso a millones de víctimas recogiendo los pedazos de sus vidas (o lo que queda de ellas).

Para hacer frente al robo de identidad y a las mentes criminales despiadadas que están detrás de él, debe tomar medidas para determinar su factor de riesgo. Saber qué información puede causar daño y con qué gravedad puede perjudicarle ayudará en la gestión de riesgos. Prevenir el robo de identidad significa proteger sus datos críticos a toda costa.

¿Qué son los datos críticos?

Los datos críticos son cualquier forma de información de identificación personal exclusiva de usted. Nunca debe compartir estos datos con nadie a menos que sea necesario y se almacenen en un lugar físico seguro, como una caja fuerte en casa o una caja de seguridad. Si llega un momento en el que tiene que compartir su información privada con una empresa, asegúrese de obtener una copia de su política de privacidad.

Datos críticos que debes mantener bajo llave:

Certificado de nacimiento
Número de seguro social
Número de Identificación del Contribuyente
Número de póliza de seguro
número de cuenta bancaria
Número de Tarjeta de Crédito
Número de carnet de conducir
Número de identificación de empleado
Su riesgo de robo de identidad depende de la información directa o “datos críticos” que un ladrón de identidad tenga sobre usted. Los delincuentes pueden utilizar los datos recopilados para comprometer sus cuentas actuales. Los ladrones pueden hacerse pasar por usted utilizando sus datos para obtener más formas de identificación o detalles laborales.

Además, existen otras formas de datos que pueden causar una cantidad significativa de daños y pérdidas cuando son comprometidos por los ladrones:

Datos físicos privados. Un ladrón de identidad utilizará “datos físicos” o cualquier información que pueda recopilar de su correo o basura como una oportunidad para obtener sus datos críticos. Cuando los investigadores quieren saber más sobre un sospechoso, lo primero que miran son los hábitos de la persona. Los ladrones de identidad conocen esta táctica y la utilizan con efectos atemorizantes.

Algunas formas de datos físicos incluyen:

Dirección residencial
La etiqueta RFID de las mascotas
Correo no solicitado (folletos)
Números de cuentas de servicios públicos como agua, gas e internet.
Estados de cuenta

Los ladrones de identidad revisarán la basura de su objetivo en busca de correo o extractos de facturación desechados. Puede proteger su información utilizando una trituradora en todo su correo antes de tirarlo. Coloque un candado en su buzón y deje siempre el correo saliente en la oficina de correos.

Datos públicos. Los datos públicos son más complicados de manejar porque la información está disponible para todos. Los ladrones de identidad utilizan datos disponibles públicamente para buscar detalles críticos que comprometan a su objetivo. Cuando los delincuentes recurren a datos públicos, ya tienen el nombre de su marca o la conocen personalmente.

==========