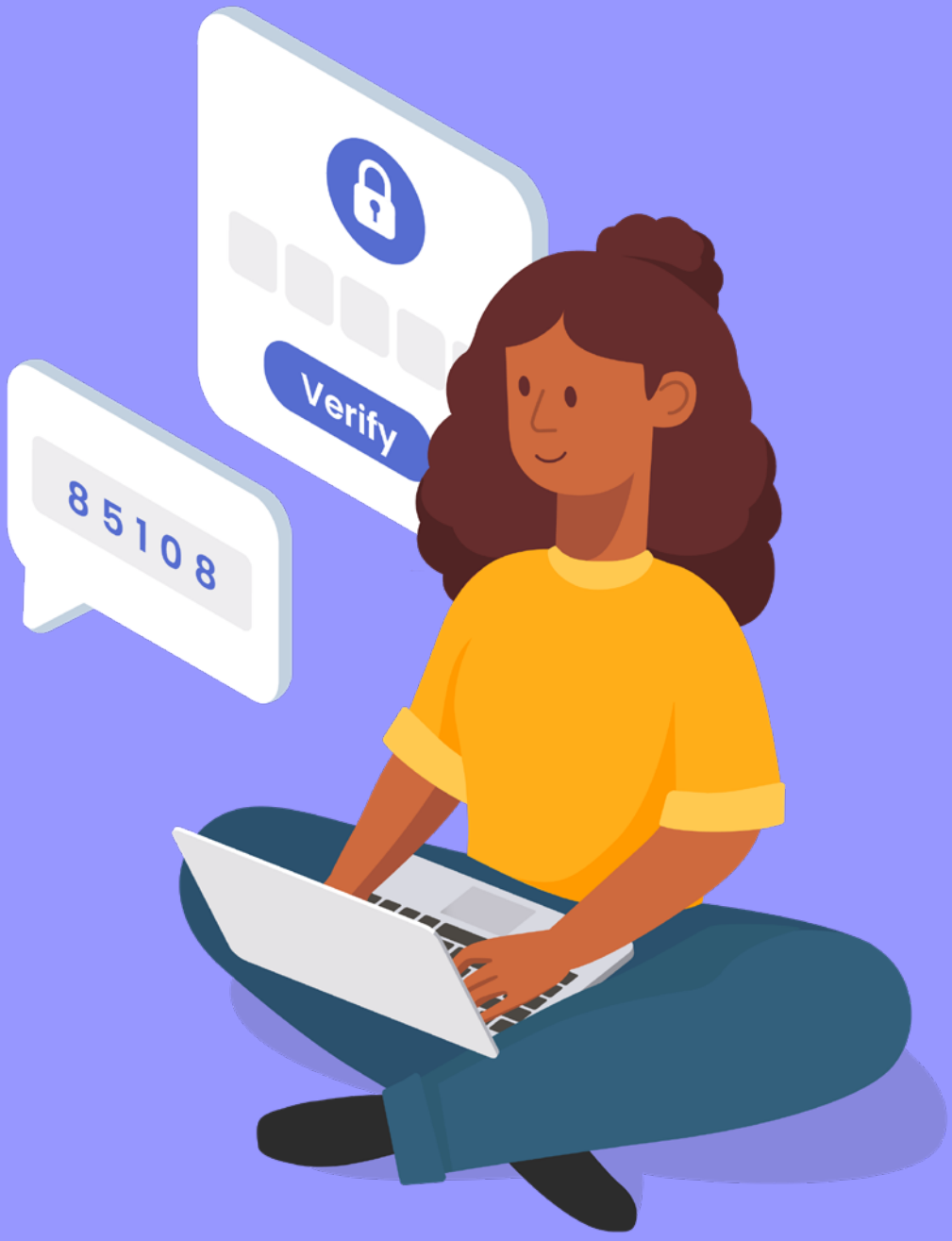
SEON



Guía

Autenticación sin fricción: Definición, ejemplos y cómo hacerla bien

SEON Technologies Ltd.
seon.io

info@seon.io
+44 20 8089 2900

Tabla de Contenidos

Las empresas en línea están en constante equilibrio entre la facilidad de uso y la seguridad. En ningún lugar es más evidente que en la fase de identificación.

¿La buena noticia? La autenticación sin fricción es posible, con las herramientas adecuadas.

¿Qué es la autenticación sin fricción?

La autenticación sin fricción es una forma de verificación de identidad automatizada basada en el riesgo. Su objetivo es aprobar a los buenos usuarios o bloquear a los usuarios de riesgo sin solicitar demasiada información personal.

Puedes implementar la autenticación sin fricción en la **incorporación digital,** el inicio de sesión o la transacción. La clave de la autenticación sin fricción es que la identificación debe producirse en tiempo real sin añadir obstáculos al recorrido del cliente.

Las formas de autenticación de clientes que se consideran de alta fricción, en contraposición a las que son sin fricción, pueden incluir:

- **verificación por video selfie**
- **autenticación multifactorial**
- **carga de documentos**
- **revisión manual de un formulario**
- **verificación del CVV y de la dirección para los pagos**

Si se eliminan estos pasos, se puede implantar una autenticación sin fricción, pero con el riesgo de aceptar más acciones peligrosas de los usuarios maliciosos. Siempre hay un toma y afloja entre la seguridad y la fricción.

La autenticación sin fricción también puede permitirte determinar si es necesaria una autenticación de usuarios adicional. Esta forma de fricción dinámica funciona como un sistema de semáforos. Permite a las empresas dejar que los usuarios de bajo riesgo sigan adelante con sus acciones. Los usuarios de alto riesgo son bloqueados inmediatamente, mientras que las acciones de los usuarios de riesgo medio pueden ser revisadas manualmente.

¿Por qué necesitamos estos métodos?

Dado que la experiencia del cliente se convierte cada vez más en el campo de batalla donde se ganan o pierden los negocios, las empresas tienen todos los incentivos para mejorar la facilidad de uso. Esto es así tanto si se trata de permitir a la gente comprar un bien o un servicio, como de incorporarse a tu plataforma o de iniciar sesión para acceder a su cuenta.

De hecho, un estudio de la plataforma de banca abierta Tink recogido por Business Leader afirma que el 88% de los consumidores abandonan una compra si se enfrentan a una fricción.

Precisamente por ello, resulta esencial verificar las intenciones de los usuarios sin añadir obstáculos.

¿Dónde se puede implementar la autenticación sin fricción?

Puedes implementar la autenticación sin fricción en cualquier etapa en la que necesites verificar con quién estás tratando. Esto puede ser:

- **La etapa de incorporación:** Cuando un nuevo usuario se registra en tu servicio, necesitas verificar quién es. En algunos casos, es un requisito legal, como en el caso de los requisitos KYC y AML. También es una buena práctica empresarial para reducir las tasas de fraude en las solicitudes.

- **La etapa de inicio de sesión:** La autenticación de clientes que vuelven a entrar en su cuenta es también primordial para las empresas online modernas. Debes poder confiar en que un extraño (o peor, un estafador) no está accediendo a la cuenta de otra persona, un proceso también conocido como fraude de robo de identidad.

- **La etapa de pago:** Los pagos son notoriamente difíciles de gestionar cuando se trata de equilibrar la facilidad de uso y la seguridad. Un gigante de la venta al por menor como Amazon, por ejemplo, llega a evitar pedir los CVV para acelerar el proceso de pago. Los pequeños comercios pueden encontrar esto difícil debido a las altas tasas de fraude de contracargo.

Al hacer estos pasos sin fricción, pero utilizando métodos alternativos para autenticar a los usuarios bajo el capó, estás manteniendo tus operaciones seguras sin afectar el viaje del usuario.

¿Cómo reducir la fricción de la autenticación de usuarios?

La autenticación y la fricción van de la mano. Para las empresas, el reto es reducir el riesgo sin ralentizar a los usuarios. Aquí hay ejemplos de herramientas que se pueden implementar, dependiendo de la etapa del viaje del cliente.

Enriquecimiento de datos en la fase de incorporación

Al identificar a los usuarios por primera vez, es crucial asegurarse de ofrecer un viaje sin problemas, incluso si tienes que realizar fuertes verificaciones KYC y AML.

Lo ideal es realizar comprobaciones previas al KYC, que pueden aliviar la carga de tus verificaciones KYC reales, ahorrando costos y trabajo manual.

Las verificaciones previas al KYC hacen maravillas con el enriquecimiento de datos. No solo se adquieren los datos adicionales en tiempo real, sino que también se puede obtener una tonelada de información basada en:

- **Una dirección de correo electrónico:** Gracias a la búsqueda inversa de correo electrónico, puedes aprender mucho sobre cada usuario. ¿Cuánto tiempo han tenido la dirección? ¿Es de un dominio de confianza? ¿Qué dice todo esto sobre quiénes son realmente?
- **Un número de teléfono:** Similar a la búsqueda de direcciones de correo electrónico antes mencionada, pero con un número de teléfono. ¿Es de un teléfono fijo o móvil? ¿A qué país apunta? ¿Usa una tarjeta SIM virtual sospechosa?
- **Una dirección IP:** Especialmente relevante para las comprobaciones AML relacionadas con los países sancionados, una dirección IP es también una gran manera de identificar posibles indicadores de alerta. ¿Está el usuario donde dice estar? ¿Está intentando falsificar los datos a través de una VPN o Tor?

- **El dispositivo del usuario:** Saber con qué tipo de dispositivo se conectan los usuarios no siempre es suficiente. La huella del dispositivo examina cientos de puntos de datos más, y te ayudará a saber cuándo alguien está tratando de falsificar sus datos, por ejemplo, utilizando un emulador.

Enriquecimiento de datos en la fase de transacción

Con la creciente normativa sobre pagos (PSD2, 3DS), cualquiera que acepte tarjetas de crédito en línea debe verificar a los usuarios lo mejor posible. Pero, ¿cómo se puede saber más sin pedir comprobaciones adicionales de verificación?

- **Correo electrónico, teléfono y búsqueda de IP:** Al igual que en la etapa de registro mencionada anteriormente, estos sencillos datos del usuario pueden revelar mucho sobre con quién estás tratando. Todo ello se obtiene en tiempo real, por lo que no es necesario pedir a tu cliente información adicional.

- **Búsqueda del BIN de la tarjeta:** Incluso los propios datos de la tarjeta de crédito pueden enriquecerse para saber más sobre el usuario. ¿Está utilizando una tarjeta de regalo o prepaga? ¿Apunta a una ubicación sospechosa (por ejemplo, lejos de la dirección de facturación o de compra)?

Enriquecimiento de datos en la fase de inicio de sesión

Análisis de IP + huella digital del dispositivo

Más efectiva para detectar los intentos de robo de cuenta o las cuentas múltiples, especialmente cuando puedes alimentar todos los datos a los algoritmos correctos (tales como las reglas de velocidad antes mencionadas)

Análisis de IP + búsqueda de correo electrónico o teléfono

Para obtener una perspectiva más clara de quiénes son tus usuarios, e incrementar la precisión de tus puntuaciones de riesgo.

La autenticación de usuarios que se conectan a tu plataforma consiste en proteger sus cuentas. Estos son los datos que debes enriquecer para conocer su verdadera identidad y sus intenciones:

- **Datos del dispositivo:** Con base en el dispositivo, las cookies y el hash del buscador, ¿has visto este dispositivo antes en tu sitio? ¿Apunta a un emulador sospechoso?
- **Datos de la IP:** ¿Lo has visto antes en tu sitio? ¿Apunta a una ubicación sospechosa?

Pero, ¿qué haces con todos esos metadatos adicionales que has conseguido enriquecer? Hay que introducirlos en el sistema de puntuación de riesgos adecuado. Veámoslo más de cerca.

Autenticación sin fricción

El módulo de prevención de fraude y enriquecimiento de datos de SEON utiliza el scoring de riesgo para evaluar los cientos de puntos de datos que recopila.

- **Enriquece todos tus puntos de datos:** SEON te permite enriquecer el correo electrónico, el teléfono, la IP, el dispositivo y los datos de la tarjeta para obtener una imagen completa de tus usuarios, incluidos sus perfiles públicos en las redes sociales, para saber quiénes son realmente.
- **Comprende el comportamiento de los usuarios con tests de velocidad:** Una vez que tengas los datos, puedes utilizarlos para entender cómo se comportan los usuarios. ¿Demasiados intentos de inicio de sesión en un plazo determinado? ¿Han introducido seis nombres diferentes seguidos al registrarse? Tú decides cómo se ve el riesgo y lo rastreas en todo tu sitio, aunque también hay prácticas reglas preestablecidas.
- **Gestiona la fricción dinámica:** Nuestro scoring de riesgo te permite aceptar, rechazar o revisar automáticamente una acción específica del usuario. Permite automáticamente a los buenos usuarios, bloquea el fraude obvio y escala la verificación solo para los usuarios de riesgo medio.
- **Mejora tu eficacia con el tiempo gracias al machine learning:** Puedes empezar en segundos con la solución de caja negra machine learning de SEON para dar puntuaciones basadas en tu sector. Y también puedes ejecutarlo como un sistema de caja blanca que aprende de tus datos históricos para construir modelos de riesgo cada vez más precisos.

Todo ello está disponible mediante una **prueba gratuita,** una completa flexibilidad de integración y sin costos de configuración o de servicio al cliente.

Preguntas Frecuentes

¿Qué es una transacción sin fricción?

Una transacción sin fricción es aquella en la que el viaje del cliente es lo más fluido posible. Esto significa reducir los obstáculos en forma de preguntas de seguridad, 2FA o métodos de autenticación adicionales.

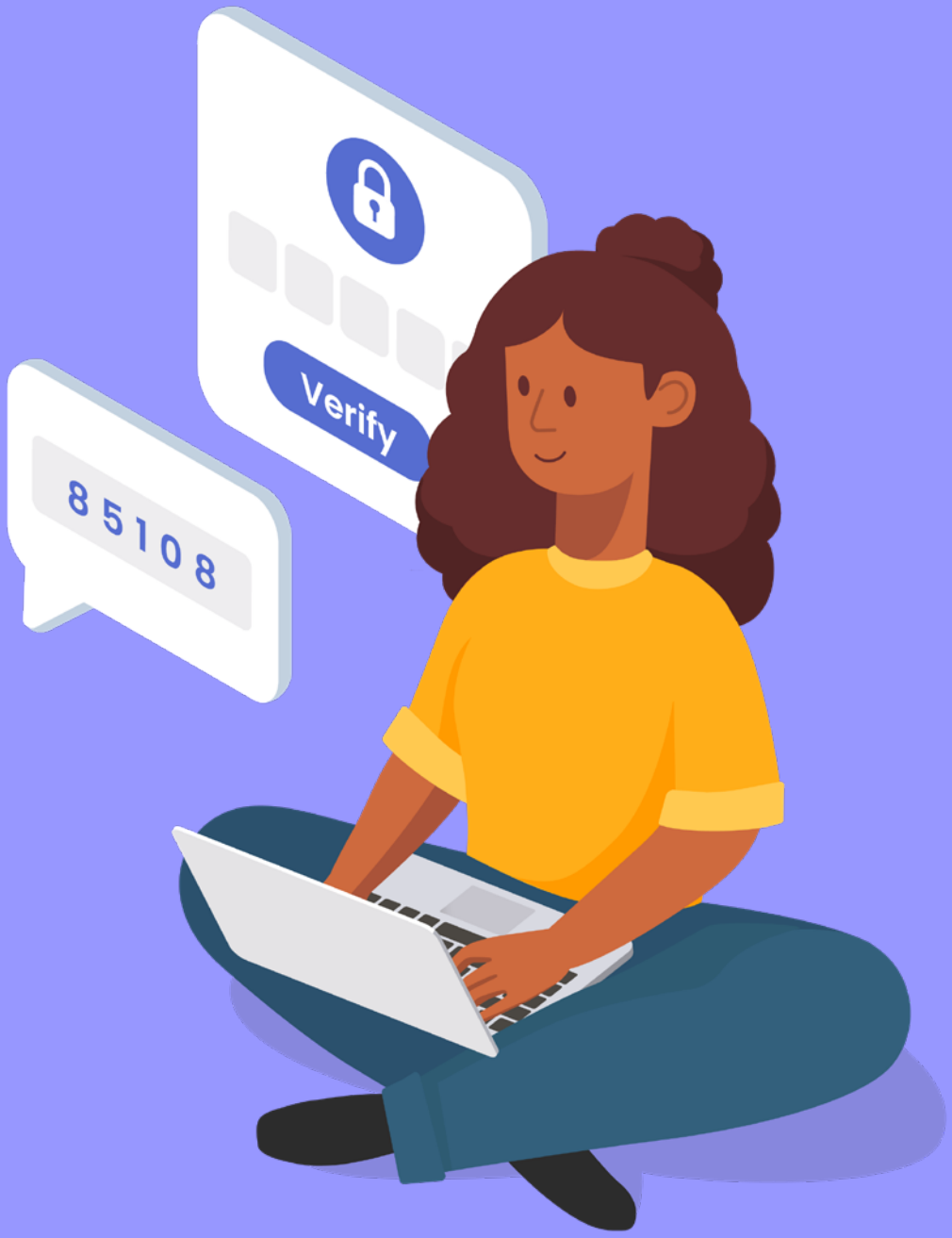
¿Qué es el inicio de sesión sin fricción?

Un inicio de sesión sin fricción se produce casi al instante sin tener que recibir códigos por correo electrónico, SMS OTP o tener que utilizar complicados métodos de autenticación multifactor. La autenticación biométrica de inicio de sesión es el método más libre de fricción.

¿Qué es el 3DS2 sin fricción?

3DS2, o **3-D Secure 2,** es una medida de seguridad puesta en marcha por las empresas de pago para reducir los pagos fraudulentos. Como la versión anterior de 3DS era notoriamente alta en fricción, la segunda actualización pretende reducirla enviando más datos entre bastidores, antes del paso de verificación real.

SEON



Para ver cómo SEON puede ayudar a su empresa a prepararse para el futuro, visite seon.io

O programe ahora una llamada de presentación de productos personalizada.

Visite nuestro sitio web

Programe una llamada

SEON Technologies Ltd.
seon.io

info@seon.io
+44 20 8089 2900