TENDENCIAS MUNDIALES DEL FRAUDE EN EL IGAMING OBSERVADAS POR SEON

SEON

¿LO SABÍAS?

La diferencia entre las 3 zonas de mayor riesgo (Asia Occidental y Central, Estados Unidos y África) y Europa es de hasta un 38% de aumento del riesgo acumulado.

Estados Unidos

- Segunda zona de mayor riesgo
- El abuso total de las primas en un solo estado puede suponer más de 18.000 USD

América Latina

- Aumento de la expansión de los operadores
- Menores costos de adquisición de jugadores
- Tasas de aprobación de jugadores un 70% superiores
- Mayor tolerancia al riesgo en los operadores de primer nivel

Reino Unido y Europa

- El mercado del juego más maduro, con operadores experimentados y tácticas de fraude más sofisticadas
- Los equipos de fraude adoptan las últimas tecnologías de prevención del fraude
- Se espera que el 25% de los nuevos jugadores sean de alto riesgo o fraudulentos
- El 64% de los jugadores se consideran legítimos en el momento del registro
- El 10% de los jugadores requieren una investigación manual antes de ser aprobados o rechazados

Asia

- Las tasas de rechazo del 40% son habituales
- La adquisición de jugadores es más barata aquí, lo que atrae a más estafadores que se aprovechan de los bonos de bienvenida
- Mayor concentración de apuestas relacionadas con criptomonedas

África

- Tercera zona de mayor riesgo

APAC y Asia

- Mercado emergente con operadores menos experimentados que reciben ataques de fraude moderadamente sofisticados y sofisticados

FRENAR EL ABUSO DE BONIFICACIONES CON LA **HUELLA DIGITAL DEL DISPOSITIVO**

Hash del dispositivo + Hash de contraseñas + IP = Los 3 puntos de datos más fuertes para conectar cuentas fraudulentas.

El hash del dispositivo, por sí solo, puede conectar a un gran volumen de jugadores.

El hash del dispositivo + IP suele detectar a los abusadores de bonificaciones menos sofisticados.

Yendo un paso más allá mediante el hash de contraseñas, rastreamos a los abusadores de bonificaciones aún más avanzados a través de numerosas cuentas.

Se trata de un simple dato al que SEON ya puede hacer referencia y que rara vez utilizan los equipos de lucha contra el fraude.

Los estafadores tienden a utilizar las mismas contraseñas, o contraseñas que siguen un patrón establecido. Esto se debe a que no es escalable para ellos crear contraseñas únicas para cada cuenta falsa.

La evolución de los estafadores ▶

Muy difícil/poco rentable de solventar

Huella digital - Correo electrónico

- Lleva mucho tiempo crear un rastro histórico detallado

Huella digital - Teléfono

- Lleva mucho tiempo crear un rastro histórico detallado

Hash de contraseña

- Lleva mucho tiempo crear contraseñas únicas para muchas cuentas falsas.

Estafadores sofisticados (profesionales de carrera)

Máquinas virtuales

- Requiere conocimientos técnicos para su instalación
- Fácil de detectar con la huella digital del dispositivo

IP única + dispositivo único

- Costos iniciales más elevados
- Difícil de detectar

Sofisticación moderada

Dispositivos únicos

- Estrategia de fraude de más rápido crecimiento
- Costos iniciales más elevados
- Difícil de detectar

Emuladores

- Requiere ciertos conocimientos técnicos para su instalación

Uso de datos móviles actualizados

- Una de las estrategias de fraude más populares
- Se utiliza con cookies de limpieza y un navegador de privacidad

Estafadores poco sofisticados

Dirección IP enmascarada

- Uso de VPN o proxies
- Fácil de crear
- Fácil de detectar

Cookies de limpieza / Navegador de privacidad

- Fácil de hacer
- Fácil de detectar con la huella digital del dispositivo

Aficionado oportunista

Nueva dirección de correo electrónico

- Muy fácil de detectar debido a la falta de huella digital

Pestaña privada del navegador

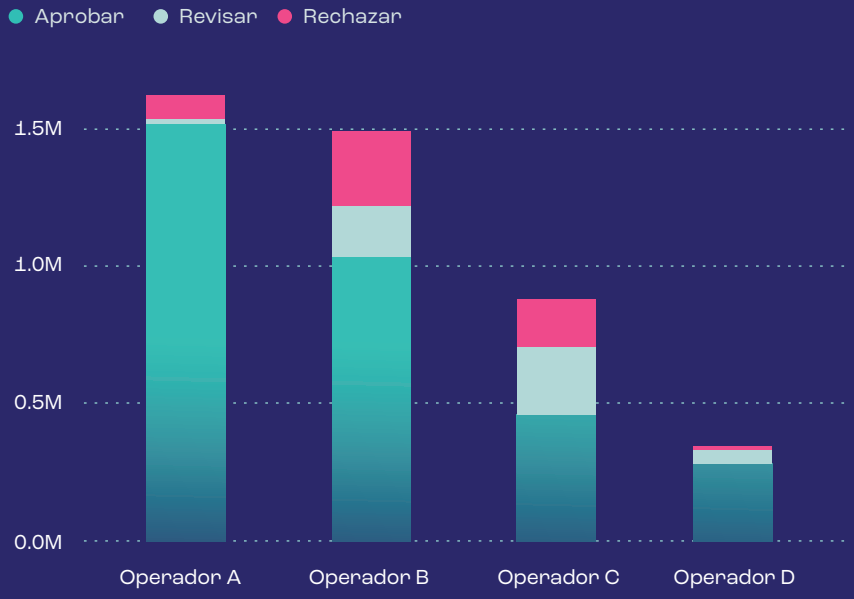
- Fácil de detectar por la huella digital del dispositivo y la falta de cookies

FRAUDE DE AFILIADOS EN LOS OPERADORES DE PRIMER NIVEL

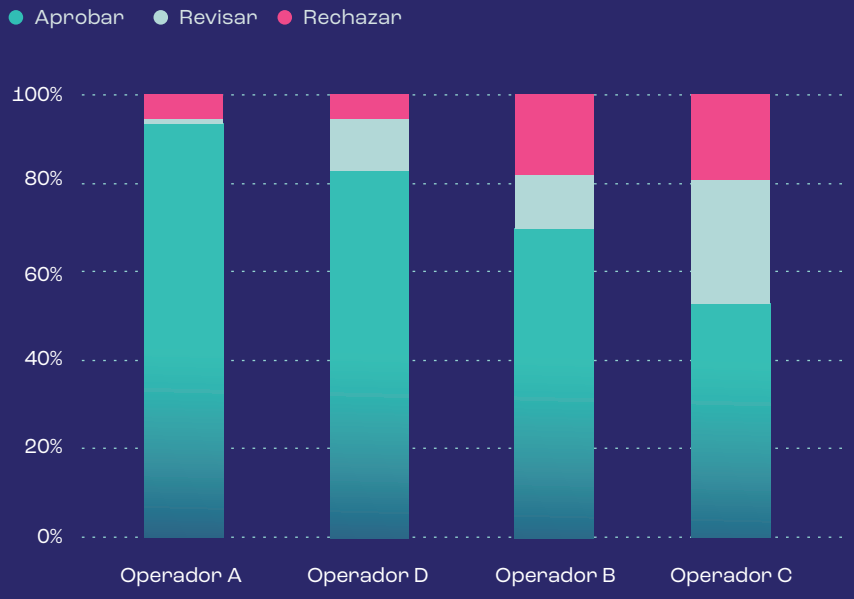
Incluso entre los operadores de juegos de azar de primer nivel, el tráfico de afiliados puede ser un éxito o un fracaso.

- En promedio, los operadores de primer nivel:
  - Aprueban el 76% de los nuevos registros procedentes de fuentes afiliadas.
  - Rechazan el 12,8% de los nuevos registros de fuentes afiliadas.
  - Realizan revisiones manuales adicionales en el 11% de los nuevos registros de fuentes afiliadas.
- Los operadores de primer nivel con las redes de afiliación con mejores resultados ven:
  - Tasas de aceptación de hasta el 90%.
  - Tasas de rechazo de alrededor del 5,5%.
- Los operadores de primer nivel con las redes de afiliados con peores resultados registran
  - Tasas de rechazo del 20%.
  - Realizan revisiones manuales adicionales en el 30% de los nuevos registros.

Número de transacciones por etiqueta y clientes



% de registros de afiliados por etiqueta y clientes



DESCUBRE PATRONES DE FRAUDE Y OPORTUNIDADES DE INGRESOS.

SEON es la prevención del fraude y la delincuencia financiera para que marcas ambiciosas como 888, LeoVegas y Kindred prosperen en un entorno digital. Con una prueba gratuita de 14 días, integración rápida y flexibilidad de pago por uso, es una forma simplificada y moderna de luchar contra el fraude.

SEON combina señales sociales con huellas digitales, monitorea AML y utiliza machine learning completamente explicable para detectar amenazas de fraude en evolución. Diseñado para empresas de alto riesgo en los sectores de iGaming, neobancos, comercio electrónico, BNPL y Web 3.0.

SEON ha prestado servicio a más de 5.000 comerciantes y ha revisado más de 1.000 millones de transacciones, ahorrando a sus clientes más de 50 millones de euros en transacciones fraudulentas. Esta empresa internacional tiene oficinas en Austin (Texas), Budapest, Londres, Yakarta y Singapur.

seon.io info@seon.io +44 20 3997 6090