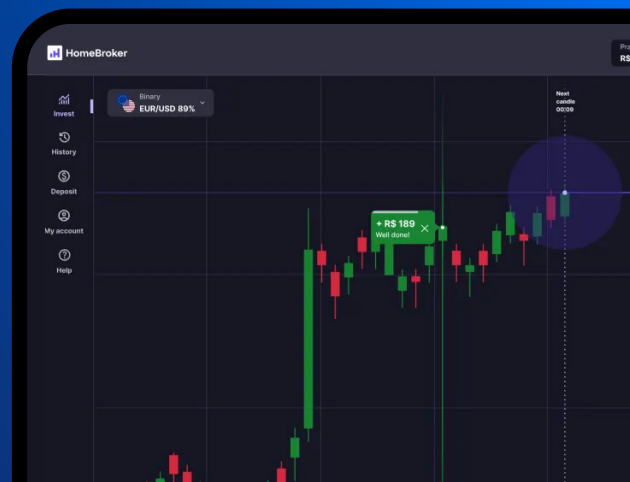


## Case Study

# Home Broker e SHIELD unem forças para aumentar confiança e segurança na negociação de opções binárias



“Os sinais de risco em tempo real fornecidos pela SHIELD têm sido fundamentais para detectar e eliminar fraudadores. Isso nos permitiu reduzir drasticamente a atividade de bots e prevenir account takeovers.”

**CEO, Home Broker**

## Key Takeaways



**92% de redução** em ataques de account takeover



**99.6%** de atividades de bot detectadas e eliminadas



Garantia de uma plataforma justa, eliminando vantagens para fraudadores

## Combater fraude é prioridade para Home Broker

No mundo acelerado da negociação de opções binárias, a promessa da Home Broker é: “Negocie em qualquer lugar, a qualquer hora”. Os usuários podem negociar ativos populares com apenas alguns cliques, prevendo se o preço de um ativo vai subir e cair. O lucro ou prejuízo vai depender da precisão das previsões dentro de um prazo selecionado.

Infelizmente, atividades de bots, contas falsas e ataques de account takeover (ATO) ameaçam a experiência dos traders. Fraudadores usam bots para executar negociações com preços desatualizados. Pior ainda, criam contas falsas para manipular mercados e roubar fundos de usuários por meio de account takeover. Essas táticas minam a confiança dos usuários e prejudicam toda a indústria.

Para enfrentar esses desafios, a Home Broker se associou à SHIELD, plataforma de risco enriquecida com inteligência artificial. Ao implementar o Device Intelligence da SHIELD, a Home Broker visa eliminar fraudes na raiz, garantindo um ambiente de negociação seguro, justo e confiável.

### Perfil do cliente

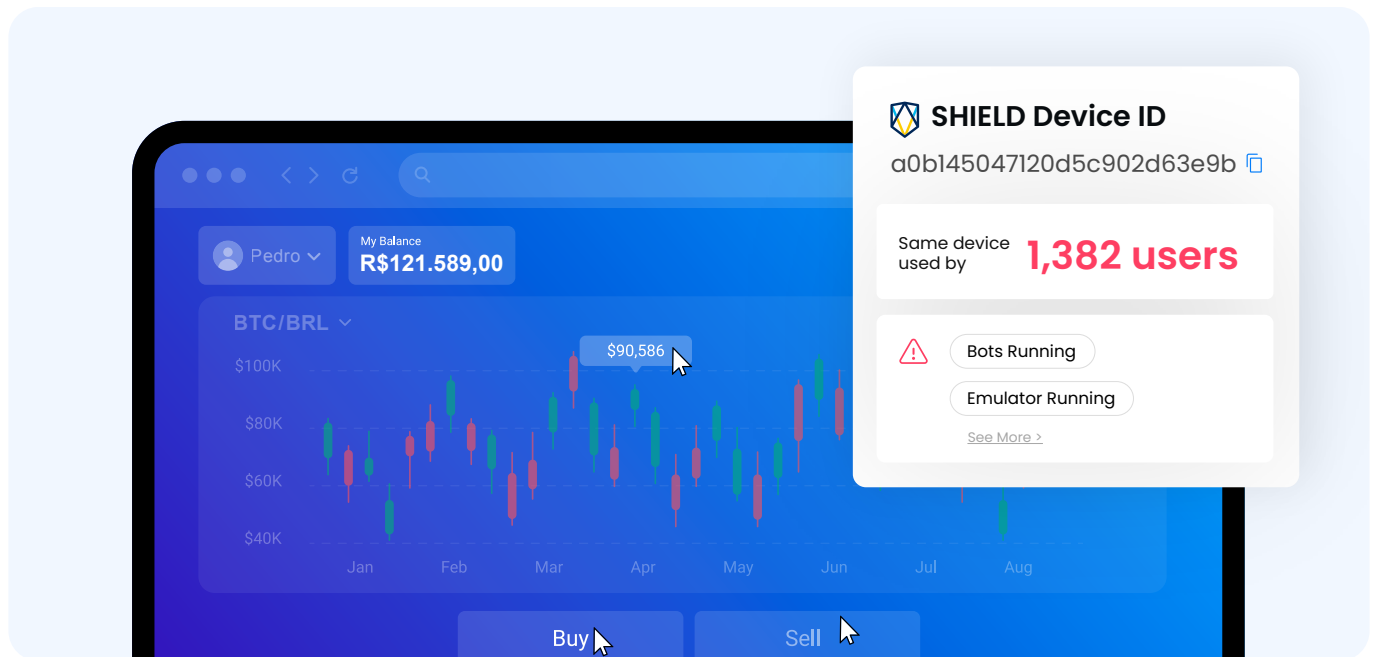
Fundada em 2023, a Home Broker é uma plataforma brasileira que torna a negociação de opções binárias fácil e simples. A plataforma permite que os usuários aproveitem todas as oportunidades de negociação de maneira acessível.

### Indústria

Serviços de trading

### Região

LATAM



## Bots & contas falsas: ameaças à confiança na plataforma

Bots que manipulam plataformas de negociação de opções binárias representam uma ameaça séria ao negócio. Aqui estão algumas táticas usadas por fraudadores para explorar os sistemas de trading:

- **Bots de negociação automatizada:** Fraudadores usam bots para realizar um grande número de negociações em rápida sucessão, explorando discrepância de preços e ineficiências de mercado para obter uma vantagem injusta em relação a traders genuínos.
- **Arbitragem de latência:** Bots aproveitam a latência no feed de dados da plataforma de trading para executar negociações com preços desatualizados. Isso permite que eles lucrem com a diferença entre o preço de mercado real e o atraso na atualização da plataforma.

Os fraudadores também criam **contas falsas** em escala usando ferramentas maliciosas, como emuladores. Eles, então, usam essas contas para negociações sincronizadas, com bots coordenando tradings para criar demanda ou oferta artificial para um determinado ativo. Essa manipulação influencia o preço do ativo, permitindo que os fraudadores lucrem com os movimentos resultantes do mercado. Além disso, contas falsas também são usadas para explorar bônus de inscrição ou de indicação e ofertas promocionais, drenando os recursos da plataforma.

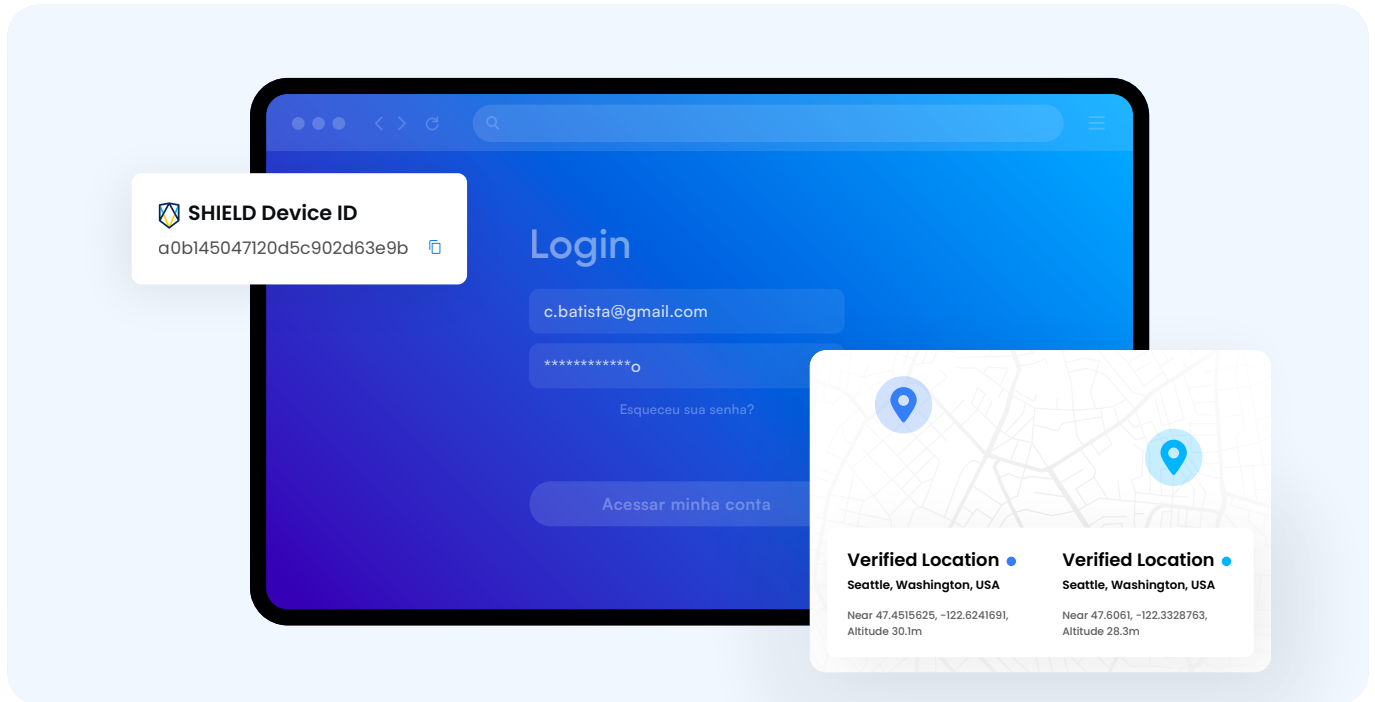
A Home Broker utiliza a plataforma de risco da SHIELD para combater esses ataques. O **SHIELD Device ID** identifica de maneira única cada dispositivo físico que acessa a plataforma da Home Broker, detectando dispositivos vinculados a múltiplas contas e atividades suspeitas.

Combinado com o **SHIELD Fraud Intelligence**, a Home Broker é capaz de monitorar continuamente cada sessão de dispositivo, detectando em tempo real o uso de ferramentas como **emuladores** e **bots** - frequentemente utilizados para manipular mercados.

## Account takeover compromete a segurança de plataformas de negociação de opções binárias

Os ataques de account takeover (ATO) também representam risco para as plataformas de negociação. Uma vez que os fraudadores conseguem acessar as contas dos usuários, eles podem realizar negociações não autorizadas, potencialmente resultando em perdas financeiras significativas para o proprietário da conta. Eles também podem resgatar fundos, 'limpando' a conta da vítima.

A Home Broker utiliza o Device Intelligence da SHIELD para impedir ataques de Account Takeover (ATO) antes mesmo que eles aconteçam. A solução consegue identificar quando há várias tentativas de login em uma única conta,



detectando, por exemplo, se a conta está sendo acessada de dispositivos diferentes do habitual. Se um cliente está tentando fazer login em localizações diferentes do que o habitual, usando devices que não são familiares, isso é um forte indicador de uma tentativa de ATO.

### Protegendo o futuro da negociação

A SHIELD ajuda a equipe da Home Broker a garantir um ecossistema confiável e justo para todos os usuários, eliminando atividades de bots e contas falsas usadas por fraudadores para manipular negociações e obter vantagens injustas. Tentativas de ATO também são identificadas e interrompidas antes que ocorram, garantindo um ambiente seguro para todos os usuários.

Impulsionada por tecnologia avançada de device fingerprinting e pelos mais recentes algoritmos de machine learning e inteligência artificial, nossa solução capacita a equipe da Home Broker a detectar e responder a padrões suspeitos em tempo real, mantendo-se à frente dos fraudadores.


“Os sinais de risco em tempo real fornecidos pela SHIELD têm sido fundamentais para detectar e eliminar fraudadores. Isso nos permitiu reduzir drasticamente a atividade de bots e prevenir account takeovers”, disse o CEO da Home Broker.

SHIELD is a device-first fraud intelligence platform that helps digital businesses worldwide eliminate fake accounts and stop all fraudulent activity.

Powered by SHIELD AI, we identify the root of fraud with the global standard for device identification (SHIELD Device ID) and actionable fraud intelligence, empowering businesses to stay ahead of new and unknown fraud threats.

We are trusted by global unicorns like inDrive, Alibaba, Swiggy, Meesho, TrueMoney, and more. With offices in San Francisco, London, Berlin, Jakarta, Bengaluru, Beijing, and Singapore, we are rapidly achieving our mission - eliminating unfairness to enable trust for the world.

For more information, visit [shield.com](https://shield.com).

 /shieldfraud

 /shieldfraud

 /company/shield

 [shield.com](https://shield.com)

