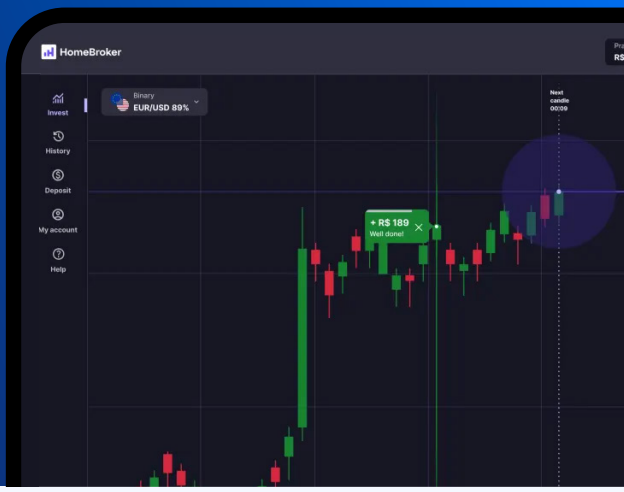
SHIELD | HomeBroker

Case Study

Home Broker and SHIELD Partner to Boost Trust and Safety in Binary Options Trading



"The real-time signals provided by SHIELD have been instrumental in detecting and eliminating fraudsters. This has empowered us to drastically reduce bot activity and prevent account takeovers."

CEO, Home Broker

Key Takeaways

92% reduction in account takeovers, safeguarding users' data

99.6% of bot activities conducted by fraudsters eliminated

Ensured a fair trading platform, eliminating advantages to fraudulent traders

Tackling Fraud Is a Priority for Home Broker

In the fast-paced world of binary options trading, Home Broker's brand promise is: "Trade on the go. Anywhere, anytime." Users can easily trade popular assets with a few taps, predicting if an asset's price will rise or fall. Their profit or loss hinges on the accuracy of their predictions within a selected timeframe.

Unfortunately, bot activities, fake accounts, and account takeover (ATO) attacks threaten this seamless experience. Fraudsters use bots to exploit pricing gaps and execute trades at outdated prices. Worse, they create fake accounts to manipulate markets and steal user funds through ATO attacks. These tactics erode user confidence and harm the entire industry.

To address these challenges, Home Broker partnered with SHIELD, the device-first fraud prevention platform. By implementing SHIELD's Device Intelligence, Home Broker aims to eliminate fraud at its root, ensuring a secure, fair, and trustworthy trading environment.

Customer Profile

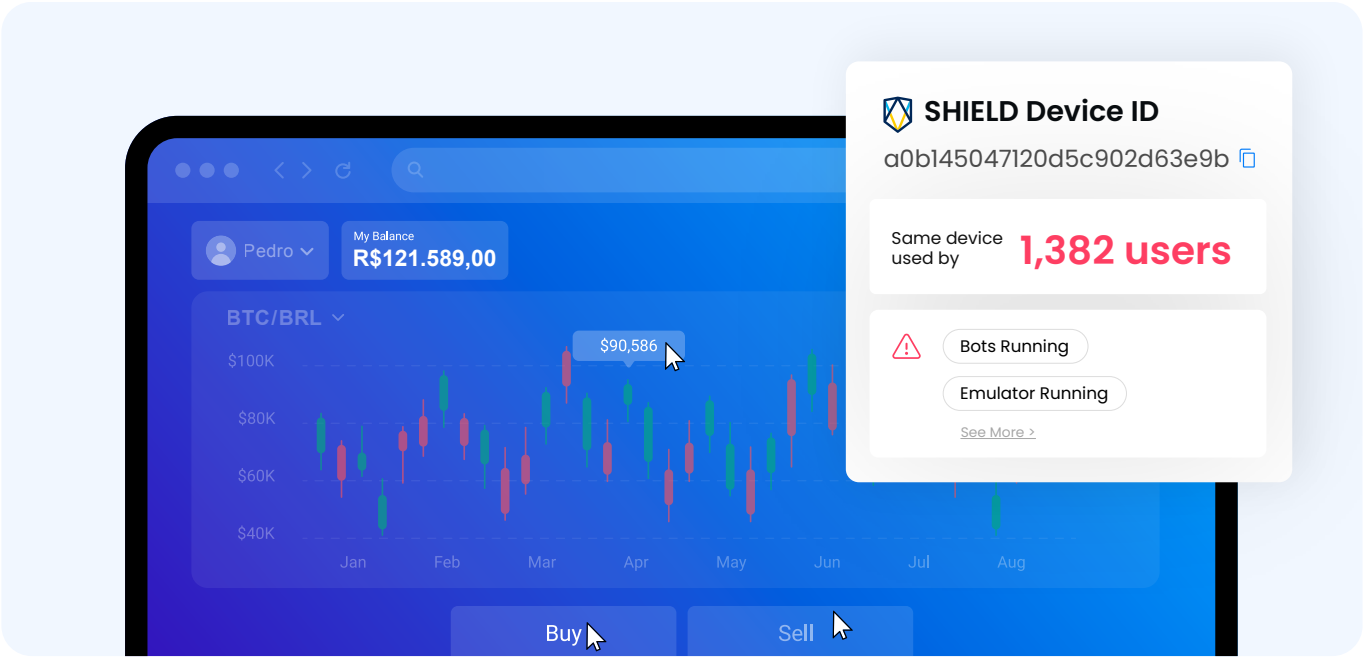
Founded in 2023, Home Broker is a Brazilian platform that makes binary options trading easy and simple. The platform allows users to seize every trading opportunity in an accessible way.

Industry

Trading Services

Region

LATAM



Bots & Fake Accounts: Threats to Trust in Trading

Bots manipulating binary options trading platforms pose a serious threat. Here's how fraudsters exploit trading systems:

- **Automated Trading Bots:** Fraudsters use automated trading bots to place a large number of trades in quick succession, exploiting pricing discrepancies and market inefficiencies to gain an unfair advantage.
- **Latency Arbitrage:** Bots take advantage of latency in the trading platform's data feed to execute trades at outdated prices. This allows them to profit from the difference between the actual market price and the delay on the platform.

Fraudsters also create **fake accounts** at scale using malicious tools like emulators. They use these accounts for synchronized trading, with bots coordinating trades to create artificial demand or supply for a particular asset. This manipulation influences the asset's price, allowing fraudsters to profit from the resulting market movements. Additionally, fake accounts are also used to exploit sign-up bonuses, referral bonuses, and promotional offers, draining the platform's resources.

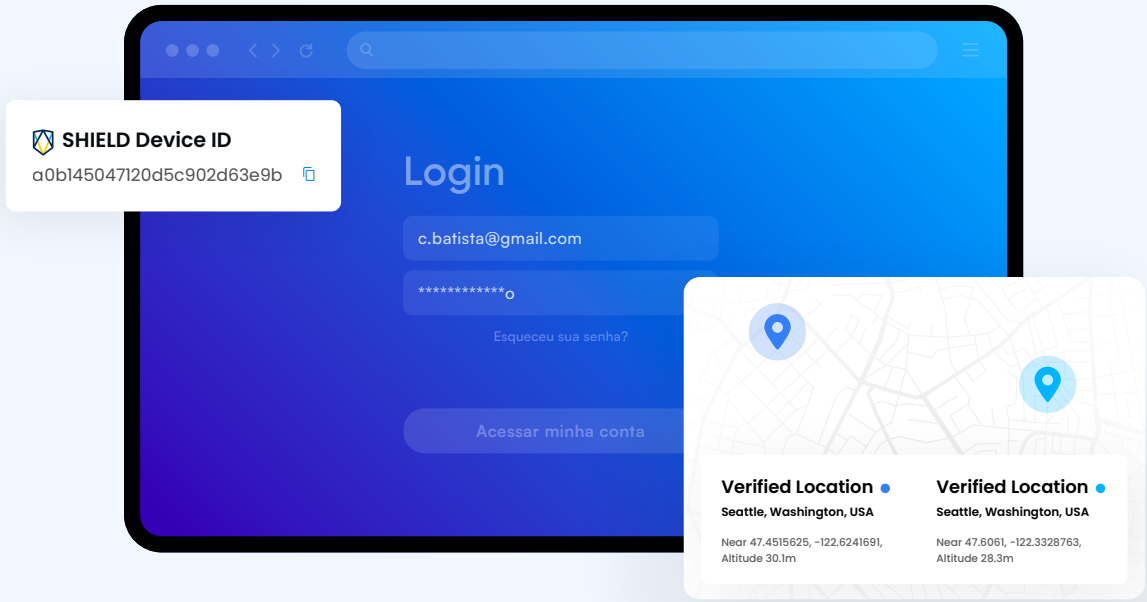
Home Broker leverages SHIELD's Device-First Fraud Intelligence Platform to combat these attacks. **SHIELD's Device ID** uniquely identifies every physical device on Home Broker's platform. Equipped with this intelligence, Home Broker's teams are able to identify when fraudsters are controlling multiple accounts, stopping coordinated trades and pump and dump schemes.

Combined with **SHIELD's Fraud Intelligence**, Home Broker is able to continuously monitor every device session, detecting in real time when the use of tools like **emulators** and **bots** - frequently used to manipulate markets.

Account Takeover Undermines The Safety of Binary Options Trading Platforms

Account takeover (ATO) attacks are another major threat to trading platforms. Once fraudsters gain access to users' accounts, they can make unauthorized trades, potentially leading to significant financial losses for the account owner. They can also withdraw funds, draining the victim's account.

Home Broker leverages SHIELD's Device Intelligence to prevent Account Takeover (ATO) attacks before they occur. The solution detects multiple login attempts on a single



account and flags suspicious activity, such as access from unfamiliar devices. If a customer logs in from different locations using unfamiliar devices, it's a strong indicator of an ATO attempt.

Shielding the Future of Trading

SHIELD helps the Home Broker team ensure a trustworthy and fair ecosystem for all users, eliminating bot activity and fake accounts used by fraudsters to manipulate trades and gain unfair advantages. ATO attempts are also identified and stopped before they happen, ensuring a safe environment for all users.

Powered with cutting-edge device fingerprinting and the latest in AI & machine learning algorithms, our solution empowers the Home Broker team to detect and respond to suspicious patterns in real time, staying ahead of fraudsters.

"The real-time signals provided by SHIELD have been instrumental in detecting and eliminating fraudsters. This has empowered us to drastically reduce bot activity and prevent account takeovers," said the CEO of 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**.

/shieldfraud

/shieldfraud

/company/shield

shield.com