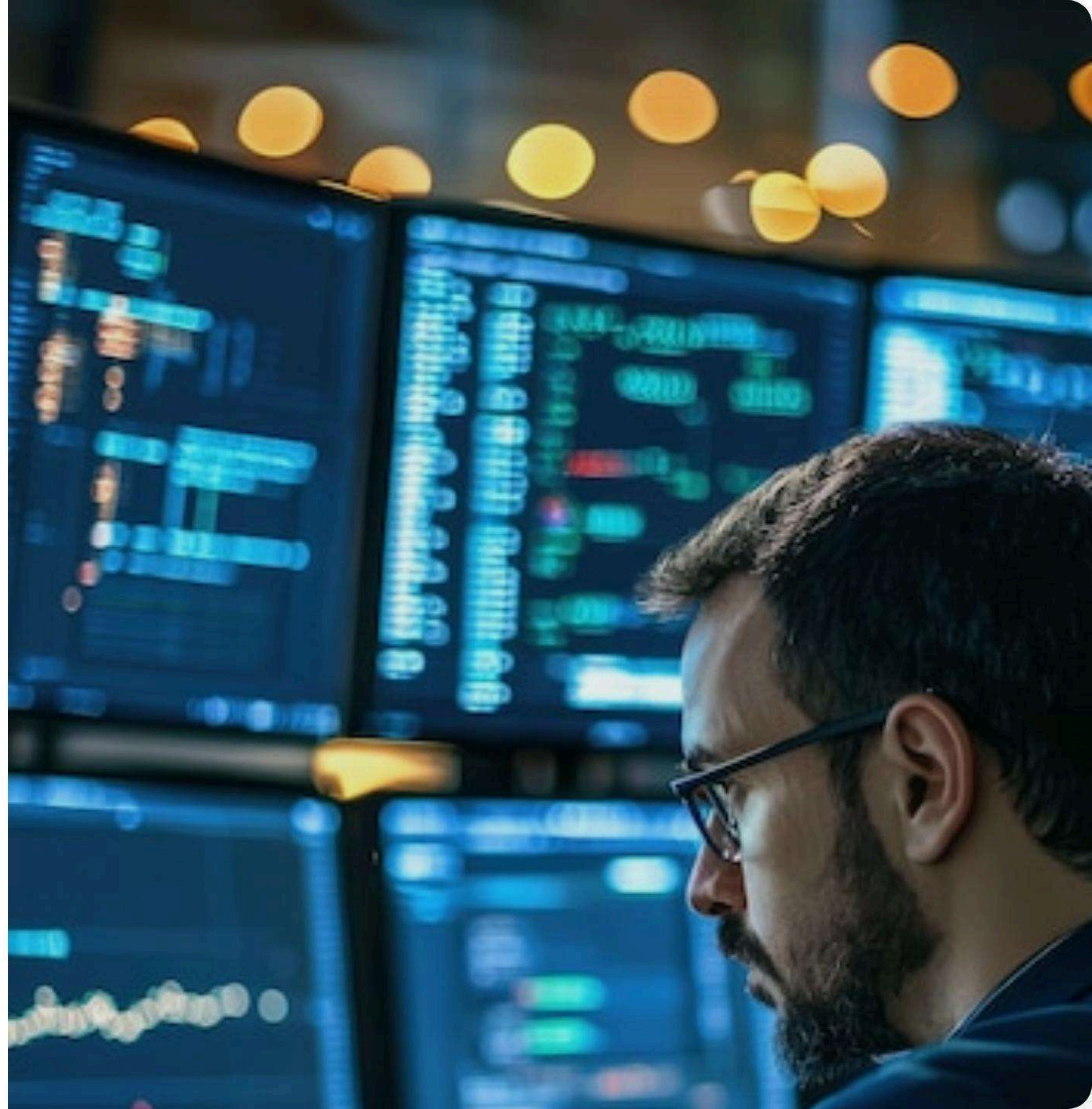


FRAUD INVESTIGATION



How Bots Skew Your Market Research Data






| The Silent Threat: Bot Contamination



15-35%

of online survey responses globally are now automated bots.

The Impact

-  **Bypass Defenses:** Modern bots beat CAPTCHAs and basic IP filters.
-  **False Data:** Internally consistent but factually false patterns.
-  **Flawed Decisions:** Strategy based on machine-generated "opinions."

| Understanding Bot Taxonomy



Simple Bots

Speed-runners. <90s completion. Straight-lining. Fail simple traps.



Hybrid Bots

Automation + Human heuristics. Pass 60% of attention checks.



AI-Trained

GPT-powered. Generate coherent text mimicking human variance.



Bot Farms

Coordinated networks using shared proxies, VPNs, and cloud services.



Identical Timing



Pattern Repetition



Semantic Plagiarism

| The Study: Tech Brand Tracking

PROJECT SCOPE

Consumer Electronics

Brand perception & purchase intent.

SAMPLE SIZE

3,847 Responses

Targeting US tech consumers.

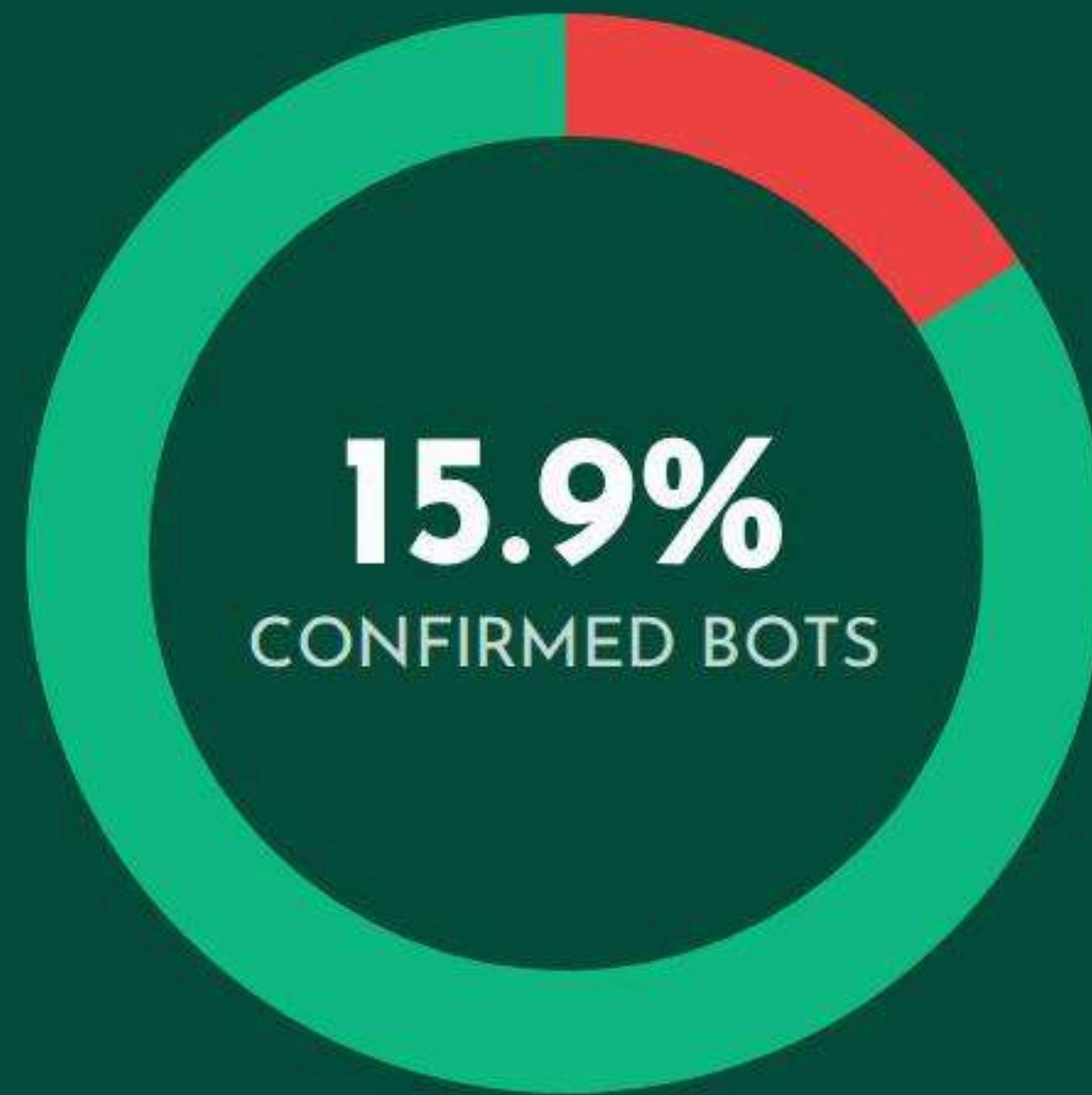
RED FLAG

22% Suspicious

847 responses flagged by platform scoring.



| Deep-Dive Analysis Results



612 Responses Discarded

 Cloud Infrastructure

68% from 3 Provider ASNs

 Response Time

Bots: 3.2m / Humans: 8.7m

 Text Analysis

55% used Templated Phrases

 Matrix Questions

Perfect Straight-Lining

| How Bot Data Nearly Derailed Strategy

Bot-Skewed Data

Brand Awareness **67% (Inflated)**

Purchase Intent **2.4x Reality**

Risk: Client planned \$2M marketing push based on false "brand strength."

Clean Data

Brand Awareness **52% (Accurate)**

Market Position **Stable**

Action: Shifted strategy to address "perception gaps" revealed by clean data.

Total ROI: \$2.45M Saved

| Building Bot-Resistant Research

Immediate Remediation

- ✓ Re-fielded 612 responses with verified panelists.
- ✓ Recalibrated all client expectations with clean dataset.
- ✓ Alerted network security partners to bot infrastructure.

Future Prevention Framework

- ✓ **Multi-Layer Detection:** Device fingerprinting & behavioral biometrics.
- ✓ **AI Defense:** Use AI models updated quarterly to match bot evolution.
- ✓ **Strict Sourcing:** Exclude cloud-hosted IPs and limit proxy usage.

