Arkose Labs

AI Accelerant to Online Fraud

Protecting business operations and customers is critical.

But the risk landscape is evolving, fueled by AI. Are enterprises equipped? Discover key trends and how leaders are responding to them from our latest research, "The Intersection of AI, Digital Fraud and Cyber Defenses."

Revenue-generating sites and apps are prime targets for attacks.

Concerned to a moderate/large extent over threats to critical business applications

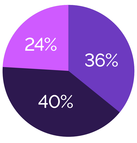
ATO/credential stuffing	76%
Fake account creation	70%
Generative AI-based threats	66%
MFA compromise	57%
Loyalty point theft/fraud	56%

TREND

AI-powered bots are on the rise and are now the most frequent source of attacks in a rapidly evolving threat landscape.

PROPORTION OF CYBERATTACKS

- Human Fraud Farms
- Basic Bots
- AI-powered Bots



TREND

More tools are in the hands of amateur fraudsters, who are targeting more companies to cash in. With a two-year head start, bad actors are leveraging AI-powered bots to boost their efficiency and maximize profits.

88% of companies report they have observed an increase in AI bot attacks.

TREND

Less than 1/4 of enterprises are ready for this onslaught.

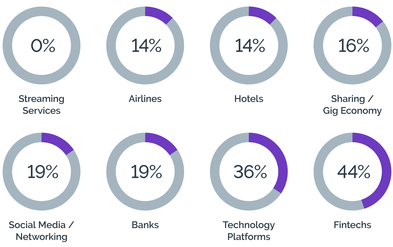
23%

of companies report being very well prepared in defending against bad actors conducting volumetric AI-powered attacks.

TREND

Which industries report they are very well prepared to defend against volumetric AI-powered attacks? The answer varies.

PREPAREDNESS BY INDUSTRY



TREND

Most companies have suffered material losses over the past two years.

53% of companies lost between $10M and over $500M.

In response, leaders are harnessing AI to defend against AI-enabled attacks.

BEST PRACTICES

1 Account takeover / credential stuffing	Leverage AI-resistant challenges that cannot be detected by adversarial AI tools.
2 MFA compromise	Enable real-time identification of reverse-proxy phishing sites during consumer log-in.
3 Generative AI abuse	Identify attempts to bypass geographical restrictions and impersonate legitimate users.

Fraud can no longer be considered a cost of doing business—it's a threat to your customer base and operational success. With volumetric AI attacks on the rise, investing in proven AI-resistant solutions is essential. Partner with Arkose Labs now to use defensive AI and reduce risk while cutting costs effectively. **Book your demo today.**

BOOK YOUR DEMO

Arkose Labs