Arkose Labs

The Great Impersonation: How Fake Accounts Are Fooling Online Businesses

Companies around the globe are grappling with a surge in fake account registrations. These cyberattacks loot your business and are a gateway for serious crimes and abuse like identity theft, money laundering, and disinformation campaigns.

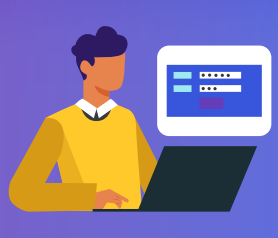
Just how massive is the problem? We dug into the data in Breaking (Bad) Bots: Bot Abuse Analysis and Other Fraud Benchmarks, Q4 2023, to find out.

The #1 Cyberattack Facing Organizations Today

In the first half of 2023, bad actors engaged in fake account creation more frequently than any other type of attack, followed by account takeover attacks and unauthorized scraping.

Fake Account Creation

Attacks connected with initial registration for an online account



ATO

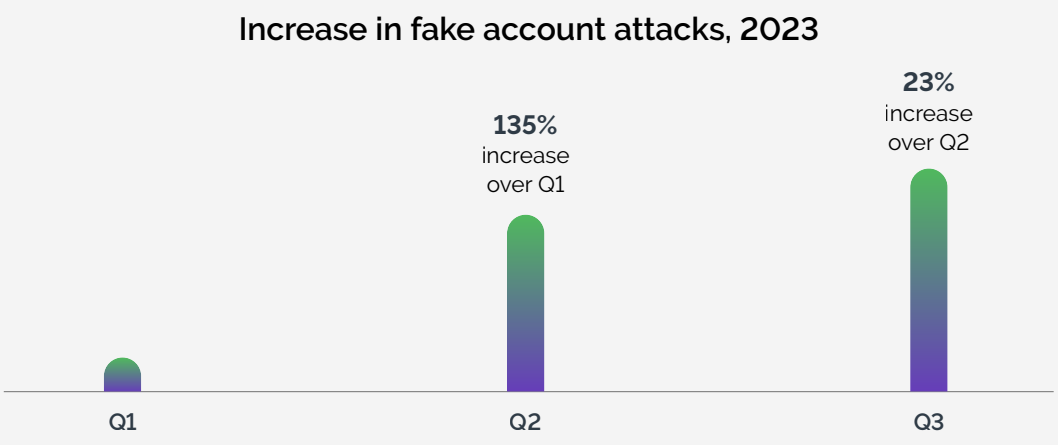
Attacks associated with logging into an account, such as ATO and credential stuffing

Scraping

The scraping of data, content, and images for malicious purposes

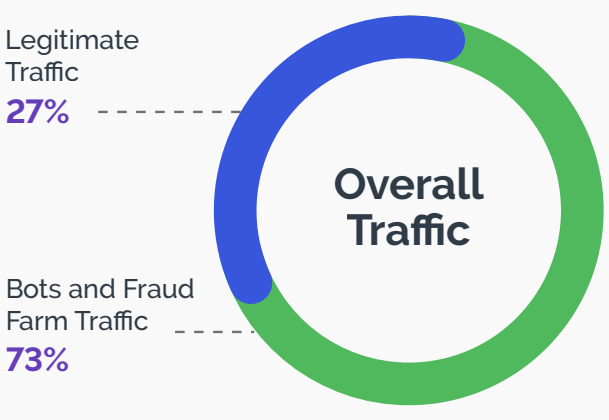
FAKE ACCOUNT CREATION IS SKYROCKETING

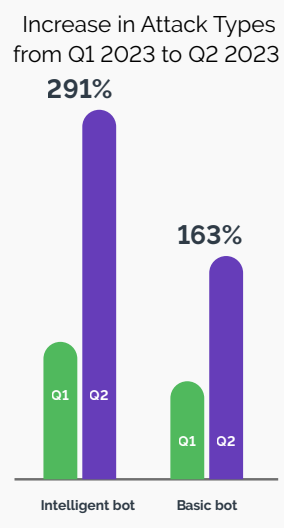
New fake account attacks are escalating at an alarming rate. They were up quarter over quarter for the first 3 quarters of 2023.



BOTS FUEL THE CYBERCRIME ENGINE

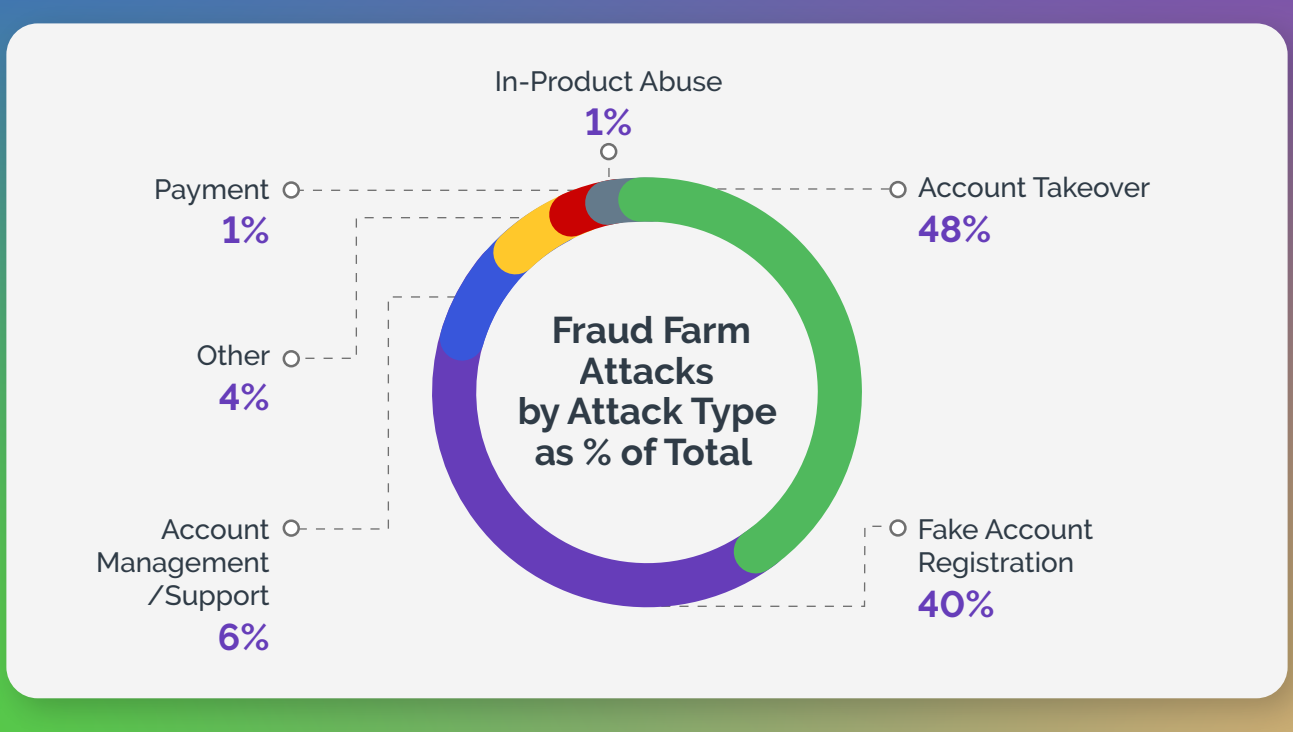
How do fake registration attacks happen? Bots are a driving force, far outpacing legitimate human traffic in overall volume online. At the same time, these automated bot tools are getting more intelligent.





HUMAN FRAUD FARMS GREASE THE WHEELS

When bots can't get through, attackers often turn to forced human labor to carry out fake account registration. When performed by humans, this type of attack is second only to account takeovers.



NO INDUSTRY IS IMMUNE

Fake account creation plagues all industries. For the first half of 2023, fake account registration was the:

#1 Attack Type For	#2 Attack Type For	#2 Attack Type when Combined with ATO For
Retail/E-commerce	Financial Services	Gift Card Companies
Social Media	Dating Sites	Streaming Media
Technology	Video Gaming	

SPOTLIGHT ON FINANCIAL SERVICES

The financial services industry is particularly at risk from fake account registration. Q2 2023 saw a 164% increase in bots attempting this cybercrime. Phony new bank accounts are likely used to launder illicit proceeds gained from real-world crimes like human trafficking, drug dealing, or weapon sales.

45%
of financial industry traffic is bad bots

164%
Increase in bot-driven fake new bank accounts

Arkose Bot Manager Stops Fake Account Creation

The Arkose Bot Manager platform provides the most effective protection against large-scale fake account registrations. Advanced risk profiling identifies suspicious sessions, while targeted enforcement challenges block automated and fraud farm-driven attacks at scale. In addition to consumable data signals for internal risk models and a global threat intelligence network, Arkose Labs offers unparalleled 24x7 SOC support and is backed by an industry-leading SLA.

Learn more about how Arkose Labs can protect your business from escalating bot attacks. Talk to an expert today.