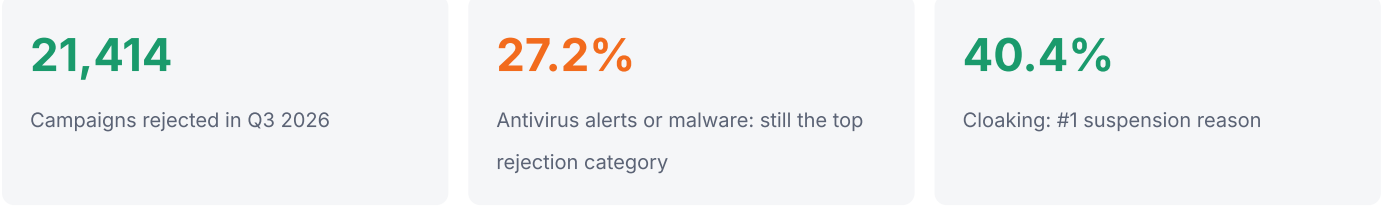


Ads Safety Report: Q3 2026

A quarterly look from PropellerAds' Policy and Security team at what is getting flagged, why advertisers get suspended, and which markets need extra scrutiny right now.



Every quarter, PropellerAds' Policy and Security team pulls together what actually happened on the platform: what got rejected, what got flagged after the fact, and where the riskiest activity is coming from. The goal is simple: give advertisers and partners a clear, honest picture of the risk landscape so everyone can plan around it.

SECTION 01

Rejected or Blocked Campaigns By Type

Platform moderation rejected or blocked 21,414 campaigns in Q3 for violating PropellerAds' rules and terms of service. That's about 3% more than in Q2 (20,790).

Rejected or Blocked Campaigns by Type · Q3 2026 · Ads Safety Report

CATEGORY	SHARE	Q2
Antivirus alerts or malware on campaign-related domains	27.2%	45.9%
Copyright	23.0%	12.5%
Other policy violations	15.6%	14.4%
Adult, pornographic, sexual, or erotic content	11.8%	5.3%
Type of content restricted in specific regions	9.2%	6.1%
False or deceptive investment advice	5.0%	4.7%
Prohibited products	3.5%	5.6%
Malware-related claims ("device infected", "viruses found", etc.)	3.0%	2.9%
Automatic file downloads	1.6%	2.6%



Malware and antivirus alerts stayed at the top of the list, but they no longer dominate it. Their share fell from 45.9% to 27.2%, which is roughly 5,800 rejections against about 9,600 a quarter ago. We still check every domain in the redirect chain, not just the landing page, so a malware flag anywhere along the way gets the campaign rejected.

Copyright was the quarter's biggest mover. It went from 12.5% to 23.0% of rejections, close to twice as many cases as in Q2 (about 4,900 against 2,600). This category covers creatives and landing pages that use brands, logos, or media the advertiser has no rights to.

Adult content rejections climbed back to 11.8% (5.3% in Q2). False or deceptive investment advice edged up to 5.0% (4.7% in Q2). Malware-related claims like "your device is infected" held steady at 3.0%.

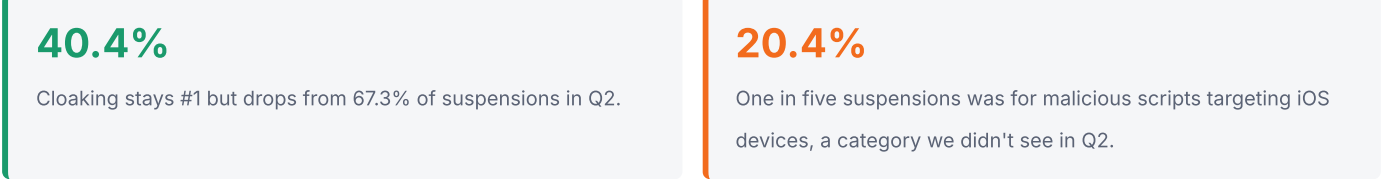
SECTION 02

Suspended Advertisers By Type

Cloaking is still the #1 reason for suspensions, but it no longer accounts for two thirds of them. Adult content and a new iOS malware category took up much of that space.

Suspended Advertisers by Type · Q3 2026 · Ads Safety Report

CATEGORY	SHARE	Q2
Cloaking	40.4%	67.3%
Adult, pornographic, sexual, or erotic content	28.5%	15.9%
Malicious scripts targeting iOS devices	20.4%	NEW
Fake tech support schemes	6.3%	4.5%
Phishing via WhatsApp and Telegram	4.4%	NEW



We suspended 270 advertisers in Q3, up from 245 in Q2. Cloaking remains the most common reason, though both its share and its absolute number went down: 109 suspensions against about 165 last quarter. It's still the main way bad actors try to show moderators one page and real users another.

Adult content nearly doubled as a suspension reason, from 15.9% to 28.5%. Together with the rise in adult rejections, this suggests more advertisers tried to submit adult offers in Q3.

"

Kate Shmeleva
Head of Business Security, PropellerAds

For a long time iOS users were seen as the harder target. This quarter says otherwise: one in five suspensions came from scripts built specifically for iPhones and iPads. Attackers clearly treat that audience as premium now, and we treat it the same way.

The new iOS category is the headline of this section: 55 advertisers were suspended for running malicious scripts aimed at iOS devices. Phishing via WhatsApp and Telegram (4.4%) also became a standalone suspension reason. Fake tech support schemes grew slightly, from 4.5% to 6.3%. Fake ID and Other violations didn't show up as separate categories this time.

SECTION 03

High-Risk GEOs

Risk doesn't spread evenly across markets. Among the GEO clusters that stood out in Q3 by the number of advertiser suspensions were China and Tier-1 markets. Turkey dropped off the list, and China is new.

🇨🇳 China (CN)

NEW ON THE WATCHLIST

China joins the watchlist for the first time this quarter. We're seeing a lot of activity from advertisers in China and the wider Asian region who try to launch campaigns that exploit iOS vulnerabilities. Our Policy team usually stops these advertisers quickly, before any campaign with malicious code can go live.

CN iOS Exploits

🌐 Tier-1 Markets

HIGH-INVESTMENT FRAUD

Bigger CPC and CPA payouts in these markets make it worth fraudsters' time to invest in serious infrastructure, such as cloaking setups, to get past tighter moderation.

US · UK · CA · AU · DE Cloaking High CPC / CPA

"

Kate Shmeleva
Head of Business Security, PropellerAds

Fraud keeps moving to wherever it's cheapest to scale. In Q3 that meant fewer mass malware landings, but more targeted attacks on iOS users and pressure from a new market, China.

SECTION 04

What to Watch in Q4

Q4 brings holiday traffic and, with it, more giveaway and prize lures. We expect prize and bonus texts to stay on the list. A few checks that can help advertisers avoid a rejection:

Rights to creatives Make sure you own or license every brand name, logo, and video you use. Copyright now drives almost a quarter of rejections.	No scare or prize wording "You won an iPhone" and "your device is infected" are prohibited no matter what the offer is.
Clean redirect chain Scan every domain between the click and the offer, including trackers and pre-landers, before you launch.	Regional rules Check whether your content is restricted in a GEO before you target it. This category grew to 9.2% of rejections.

CONCLUSION

Our Commitment to Ads Ecosystem Safety

Fraud tactics don't stay still, so neither can we. We keep refining how we moderate and lean on the data itself to catch new patterns early, all with the goal of keeping things safer for advertisers and users alike.

Expect more of these reports going forward. Keeping the market informed on what we're seeing is how we help partners plan around the risk landscape instead of getting blindsided by it.

🔍 Proactive Monitoring

Spotting new fraud tactics before they scale up.

🛡️ Multi-Layer Defense

Pairing automated detection with human moderation review.

📊 Data-Driven Insights

Sharing what we're seeing through regular open reporting.

🤝 Ecosystem Transparency

Earning trust by being upfront about risks and how we handle them.