Q2 2024 Ad Quality Report

User Protection and Malvertising Trends

GeoEdge's Ad Quality Report examines the prevalence and origins of malvertising attacks on global devices across programmatic advertising channels. Here's how AdTech fared in Q2 2024:

- Auto-redirects account for 40% of all malvertising attacks, up from 25% in Q1.

- In the US, weapons and politics now represent 12% and 10% of blocked content, spurred by the influx of sensitive material.

- Election ads emerge as gateways for malvertising attacks leveraging misleading product offers and financial scams to defraud users.
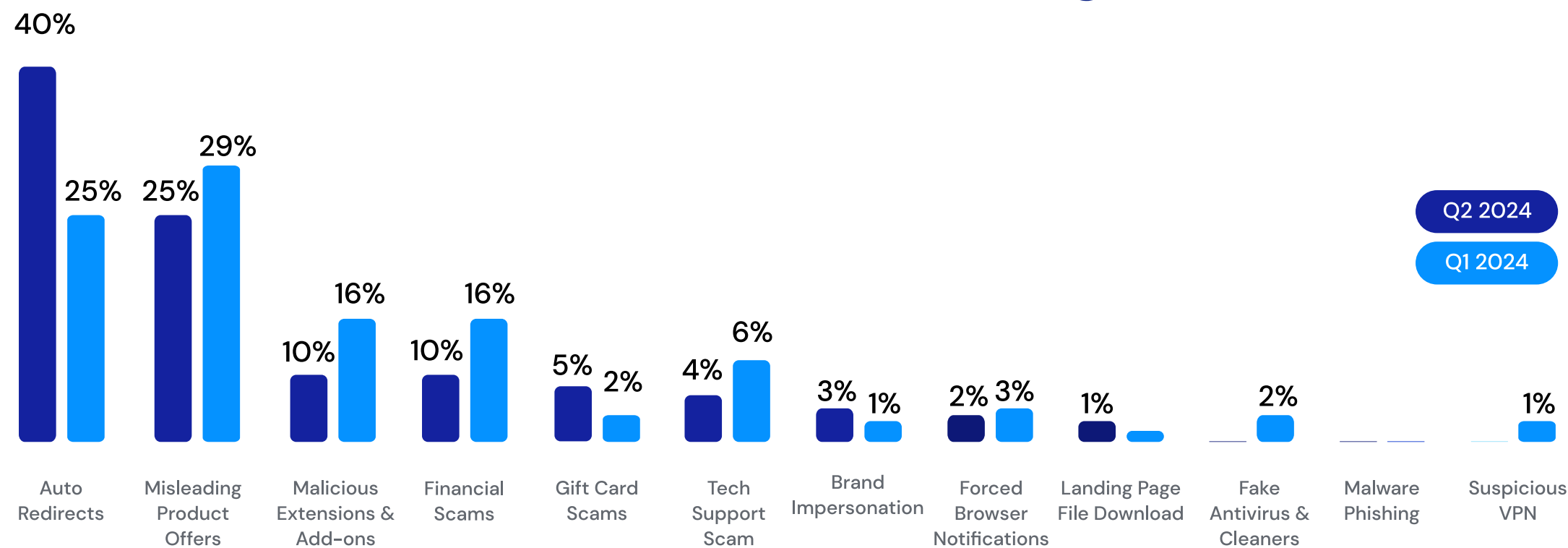
GeoEdge monitored and analyzed billions of advertising impressions across premium websites, apps, and SSPs to compile the research presented in this report. The data was collected using GeoEdge's real-time ad security solution, which assesses ad quality and malvertising blocking on live impressions across devices and channels.

Top Malvertising Attack Vectors in Q2 2024

Auto-redirects emerged as the leading threat in malvertising attacks, increasing significantly from 25% in Q1 to 40% in Q2. The other 60% of threats were driven by **clickbait scams,** with **misleading product offers** remaining the most common, though they decreased slightly to 25% from 29%. Brand impersonation and gift card scams rose this quarter.
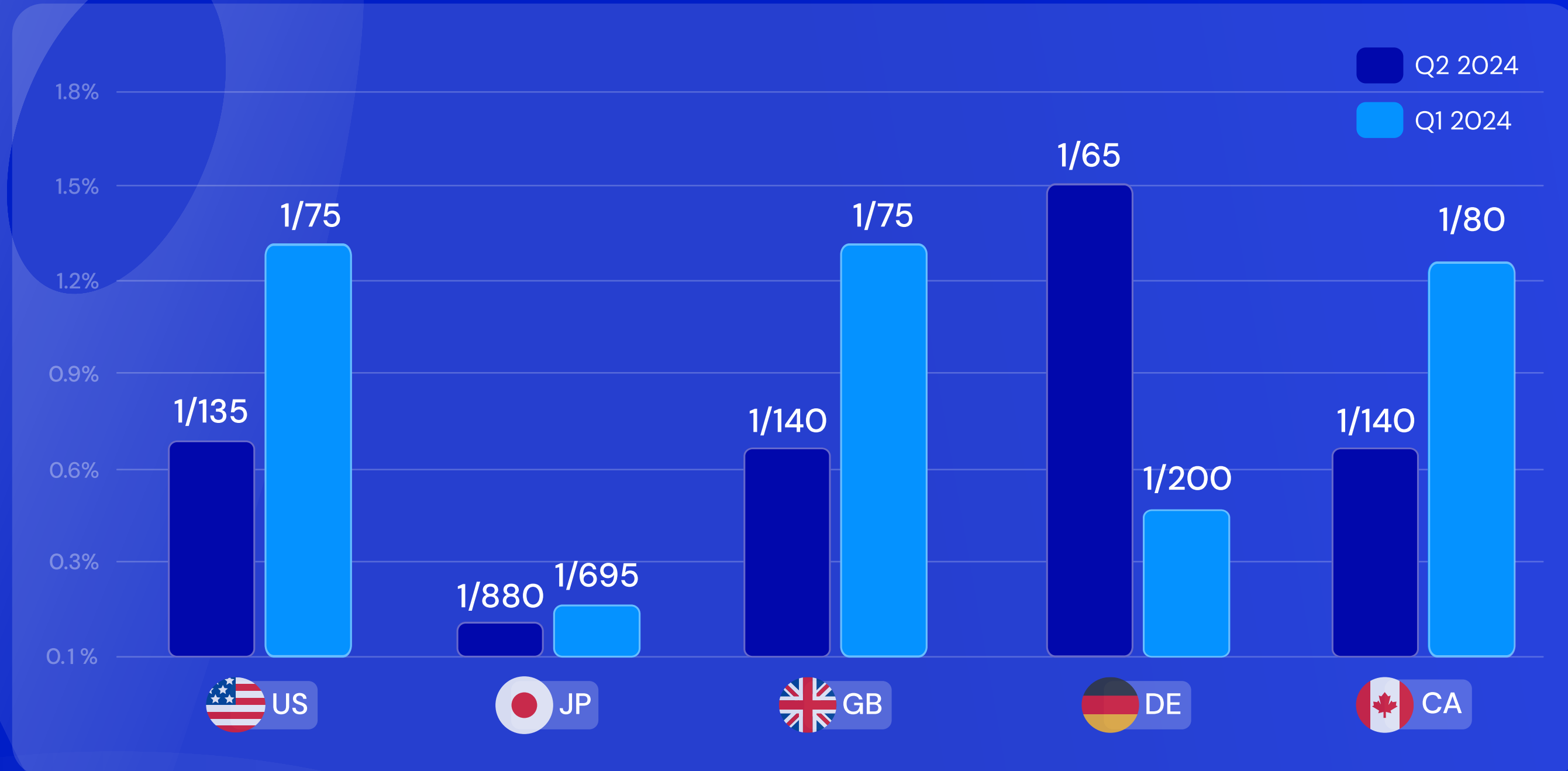

- 40%
- 25%
- 10%
- 10%
- 5%
- 4%
- 3%
- 2%
- 1%
- 0%

Legend:
- Auto Redirect
- Misleading Product Offers
- Malicious Extensions & Add-ons
- Financial Scam
- Gift Card Scam
- Tech Support Scam
- Brand Impersonation
- Forced Browser Notifications
- Landing Page File Download
- Fake Antivirus & Cleaners
- Malware Phishing
- Suspicious VPN

Malvertising Vectors: Q1 vs Q2 2024

Vector	Q2 2024	Q1 2024
Auto Redirects	40%	25%
Misleading Product Offers	25%	29%
Malicious Extensions & Add-ons	10%	16%
Financial Scams	10%	16%
Gift Card Scams	5%	2%
Tech Support Scam	4%	6%
Brand Impersonation	3%	1%
Forced Browser Notifications	2%	3%
Landing Page File Download	1%	
Fake Antivirus & Cleaners		2%
Malware Phishing		
Suspicious VPN		1%

Election Ads Emerge as Gateways for Malvertising Attacks

Threat actors are seizing programmatic channels, spreading 2024 Election-related creatives that facilitate financial scams and misleading product offers

Regional Malicious Activity

Legend: Q2 2024, Q1 2024

Country	Q2 2024	Q1 2024
US	1/135	1/75
JP	1/880	1/695
GB	1/140	1/75
DE	1/65	1/200
CA	1/140	1/80

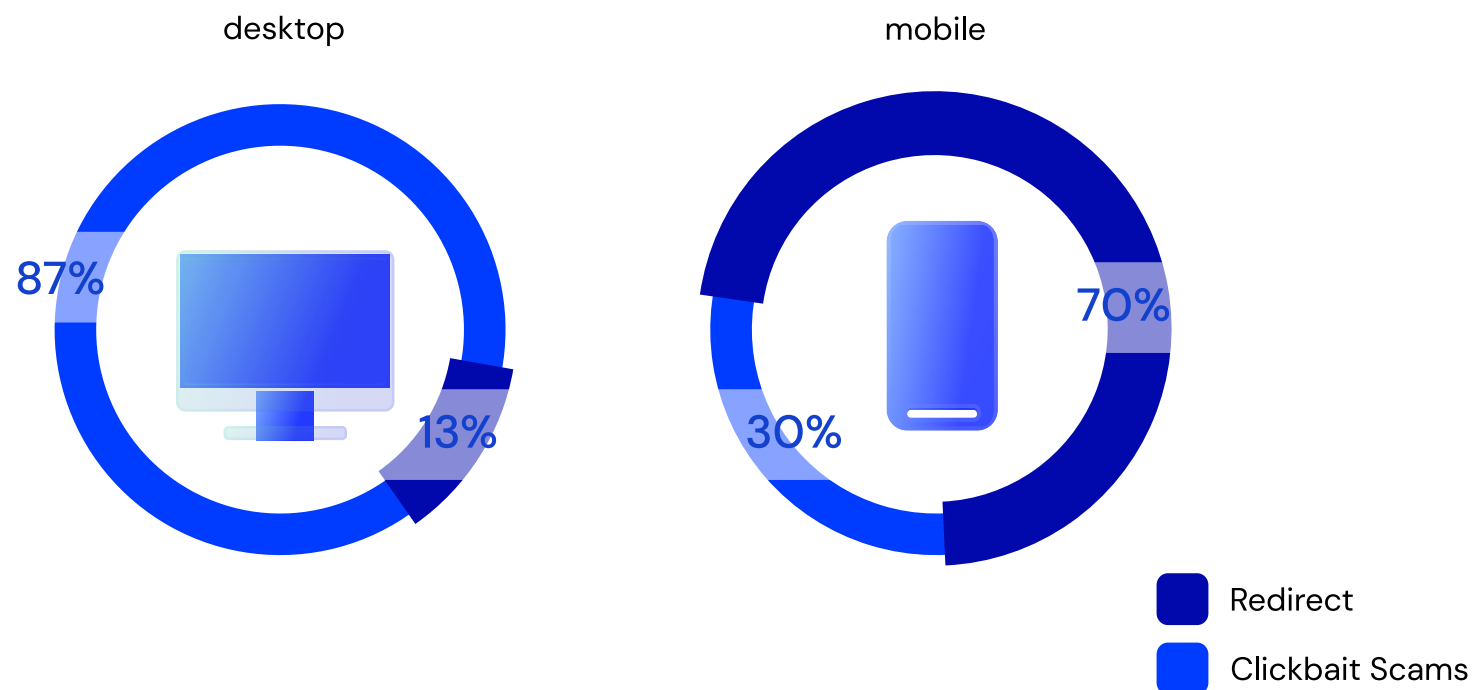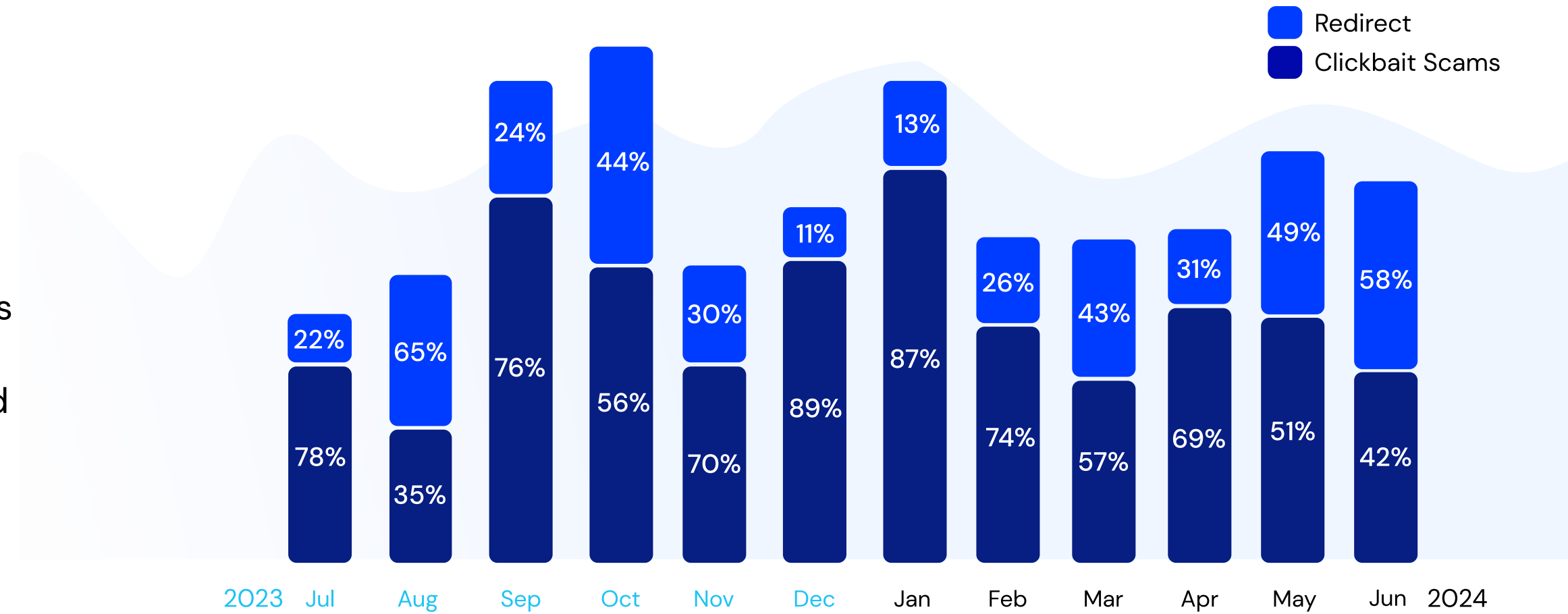Y-axis values: 0.1%, 0.3%, 0.6%, 0.9%, 1.2%, 1.5%, 1.8%

Our analysis of the five focus countries revealed a striking trend: While malvertising rates declined in the US, UK, Canada, and Japan this quarter, they surged dramatically in Germany. One in every 65 ad impressions led to a scam in Q2. 70% of these were misleading product offers, with a notable spike throughout the quarter. Financial scams accounted for 21% of malicious ads overall.

Redirect vs Clickbait Scams

Redirect vs Clickbait Scams:

The monthly trendline showed a clear rise in redirects during Q2. Although overall malvertising volumes stayed relatively steady, the share of redirects surged from 31% in April to 49% in May, reaching a dramatic 58% in June.


Legend: Redirect / Clickbait Scams

	2023 Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun 2024
Redirect	22%	65%	24%	44%	30%	11%	13%	26%	43%	31%	49%	58%
Clickbait Scams	78%	35%	76%	56%	70%	89%	87%	74%	57%	69%	51%	42%

Device Targeting

desktop — 87% / 13%

mobile — 70% / 30%

The split between mobile and desktop malvertising attacks remained steady compared to previous quarters, although the nature of the attacks shifted significantly. On mobile, auto-redirects surged to 70% of all attacks, up from 53% in Q1. Although redirects also increased on desktop devices, they were far less dominant, representing just 13% of attacks, with the overwhelming majority (87%) being clickbait scams.

43%

47%

11%

Legend: Redirect / Clickbait Scams
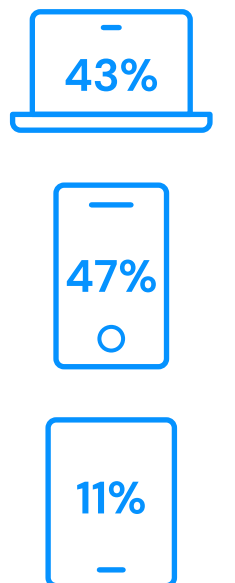
Global SSP Rankings: Malvertising Rates and Malicious Activity
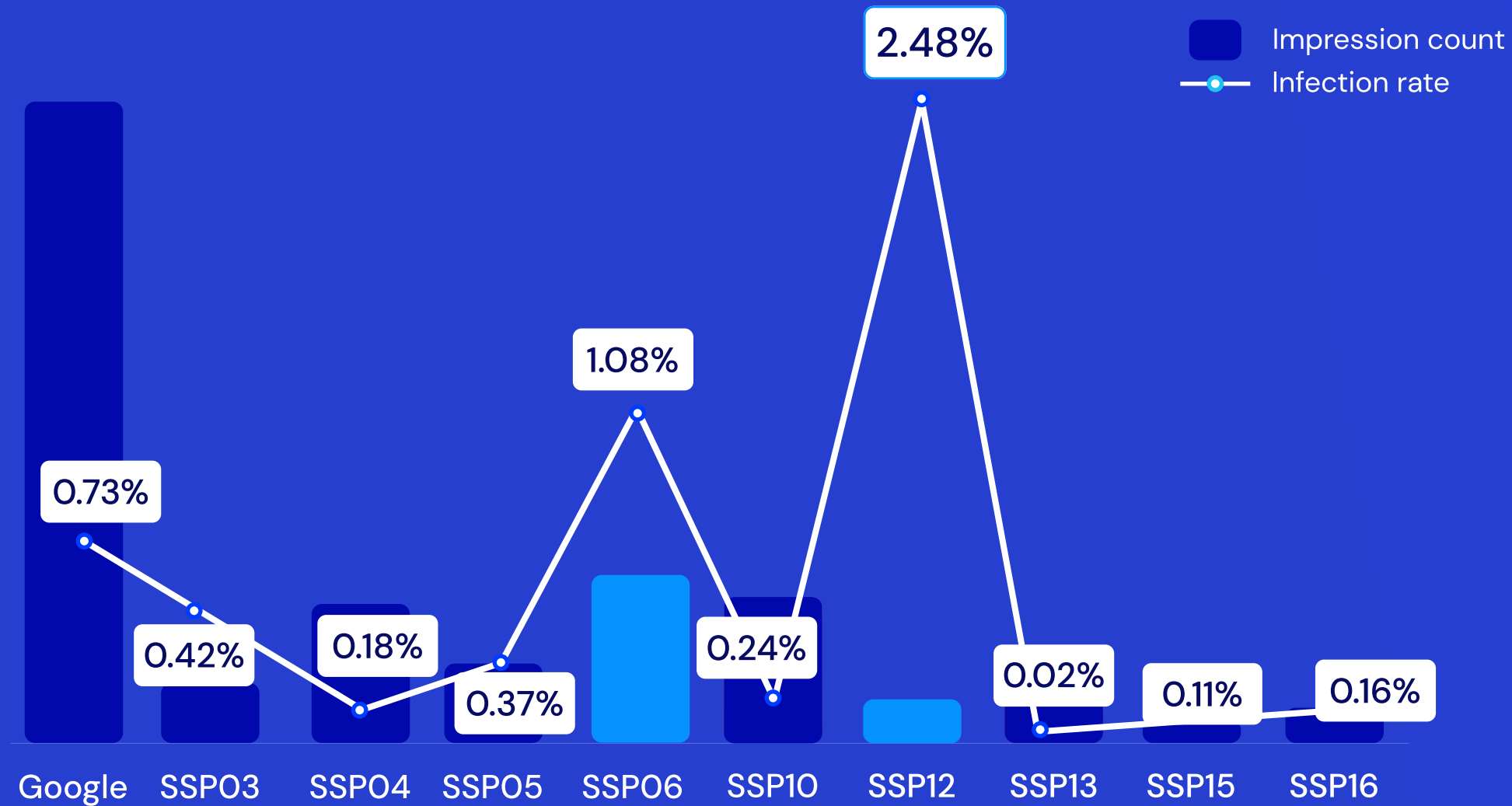
Google's Q2 malware infection rate of 0.73% remains dangerously above average, with only a slight improvement from Q1.

SSP06's malware rate improved significantly, dropping from 2.88% in Q1 to 1.08% in Q2, though this rate is still relatively high for a top 5 global SSP.

SSP10 successfully reduced its infection rate to 0.24% after experiencing a spike in Q1. SSP12 continues to pose a concern, with a low quality score and an infection rate of 2.48% in Q2, indicating that one in every 40 ads served is affected by malvertising.

Learn More >

Ad Content Filtering Trends

Gambling continued to be the most widely blocked content category across all regions, representing 65% of all blocked ad content across the EU. Tobacco, which was the second most blocked category in APAC, rose to second place in the US and Canada after not appearing in the top ten in Q1. Weapons and politics followed closely behind, accounting for 12% and 10% of blocked content. App Store categories entered the top ten blocked content categories in APAC for the first time, most notably in Japan.

The Comics category in the Google Play Store accounted for 9% of all content blocking, placing it in the third position, while the Games category in the App Store accounted for 3%. In the EU, two ad categories saw notable increases: News and Media rose from 2% in Q1 to 12% in Q2, and Weight Loss increased from 6% to 10% this quarter.

US & CA

- 36%
- 13%
- 12%
- 10%
- 8%
- 6%
- 4%
- 4%
- 3%
- 3%
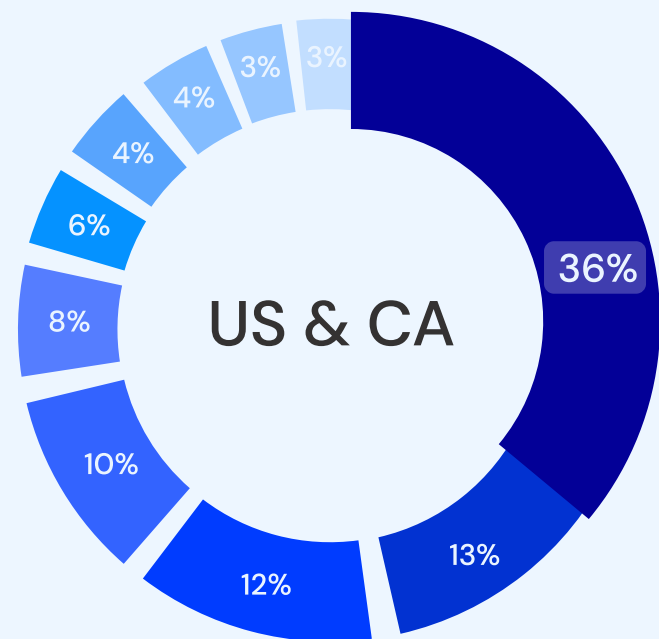
Legend:
- Gambling
- Tobacco
- Weapons
- Law, Government & Politics
- Marijuana
- Weight Loss
- News and Media
- Pharmaceuticals
- Religion
- Health

EU

- 65%
- 12%
- 10%
- 3%
- 3%
- 2%
- 1%
- 1%
- 1%
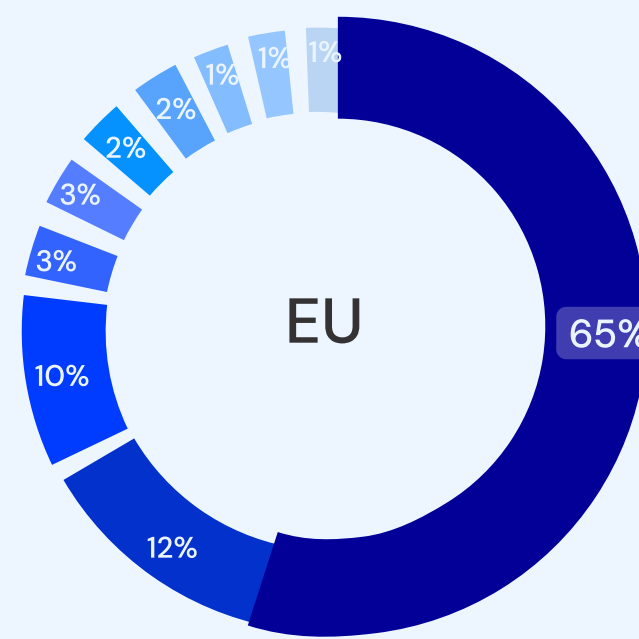
Legend:
- Gambling
- News and Media
- Weight Loss
- Swimwear and Intimate Apparel
- Health
- Tobacco
- Law, Government & Politics
- Election
- Weapons
- Religion

APAC

- 44%
- 27%
- 9%
- 5%
- 3%
- 3%
- 3%
- 2%
- 2%
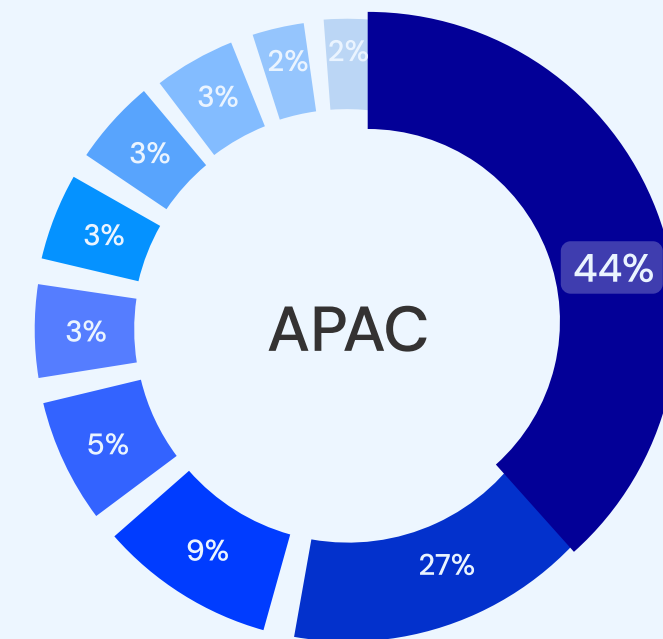
Legend:
- Gambling
- Tobacco
- Google Play Category – Comics
- Weapons
- Religion
- App Store Category – Games
- Cryptocurrency
- Swimwear and Intimate Apparel
- Pharmaceuticals
- Law, Government & Politics

Ensure User Protection and Immersive Ad Experiences with Advanced Quality Control

GeoEdge's robust ad security and user protection solutions empower publishers and platforms across web, CTV, and in-app environments to proactively block malicious actors and harmful ads. With GeoEdge, you can ensure that every ad is malware-free and meets the highest technical and content quality standards before it reaches your users. By identifying threats at the pre-impression level, we help you maintain clean campaigns and safeguard the user experience.

Trusted worldwide, GeoEdge provides real-time protection that upholds integrity and fosters trust across the AdTech ecosystem. Safeguard your audience with real-time defenses that prevent malvertising and unwanted content from disrupting the user experience.

Learn More: www.geoedge.com