2024 Ad Quality Report

Ad Quality 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 2024:

- **Over 70% of users view at least half of online ads as untrustworthy, driven by a 10% year-over-year increase in malvertising levels in 2024.**
- **Mobile users faced 56% of malicious ads, with 68% of these attacks involving redirects.**
- **Canada reported malvertising appearing in 1 out of 75 impressions, while Germany saw a 45% increase in malicious activity.**

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.

Malvertising Trends Q4 2024

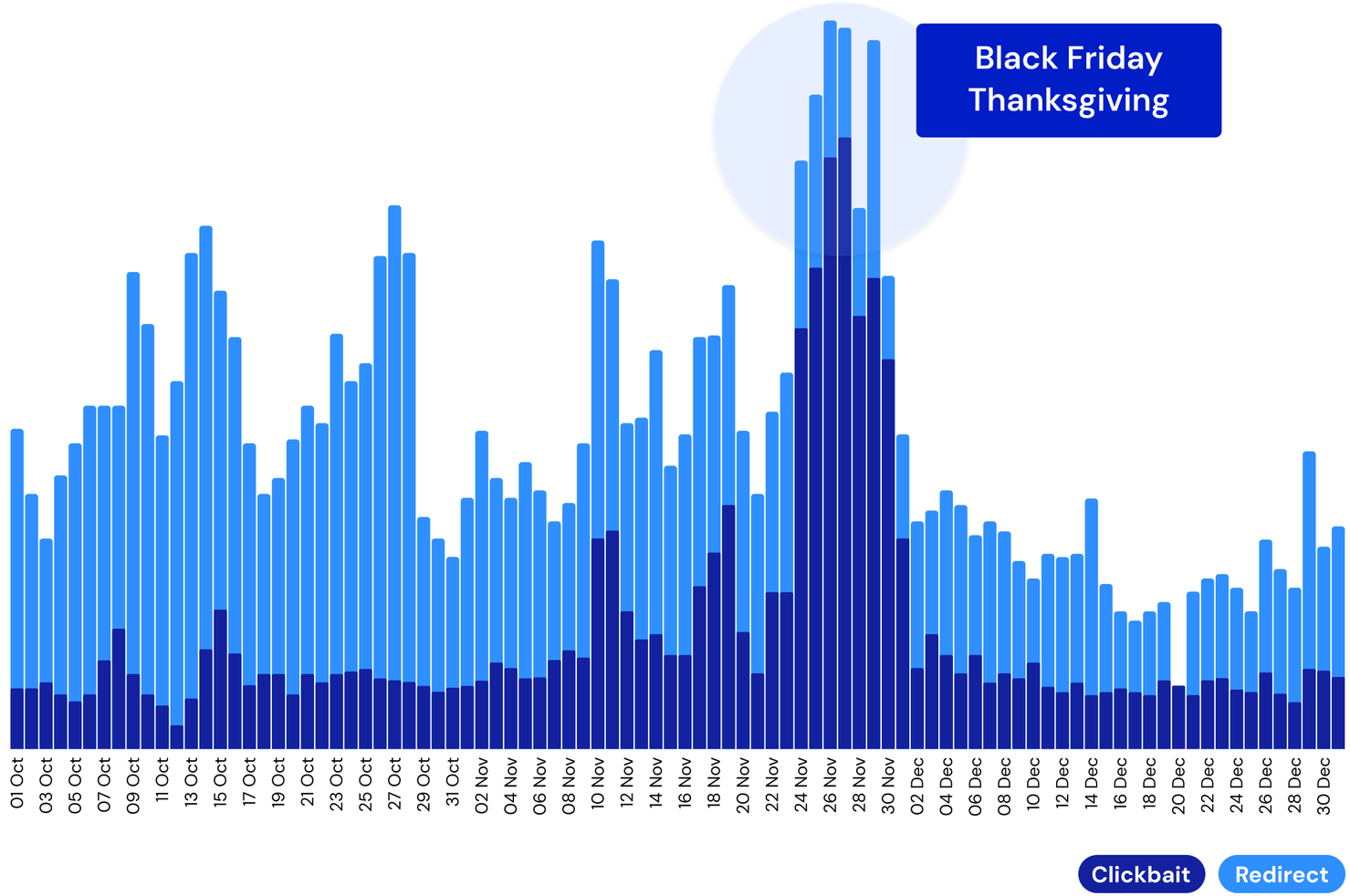
Holiday Clickbait Dominates Q4

Over 70% of users now perceive at least half of online ads as untrustworthy—a trend fueled by a 10% year-over-year surge in malvertising levels in 2024. Malvertisers are increasingly exploiting social engineering tactics to deceive users, with holiday shopping events like Thanksgiving and Black Friday fueling a surge in clickbait scams.

The primary scams identified include:

Misleading product offers: 31%
Tech support scams: 23%
Financial scams: 22%

Learn More

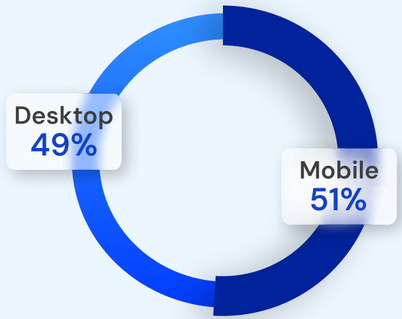


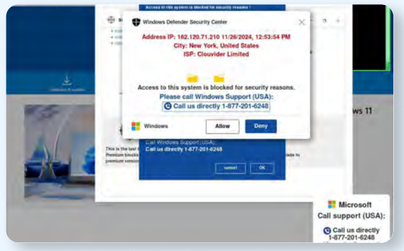
Q4 Malvertising Clickbait Attacks

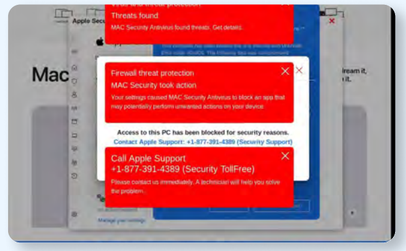
The Holiday Season's Hidden Threats

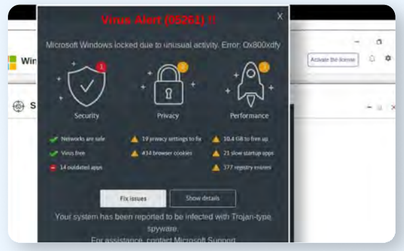
Tech Support Scams

Malicious Domain:
web.core.windows.net





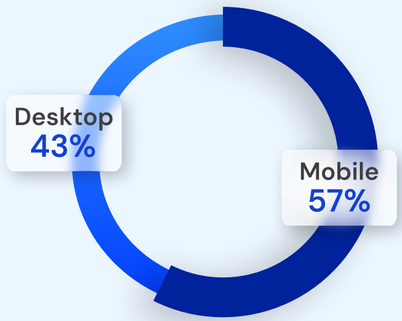


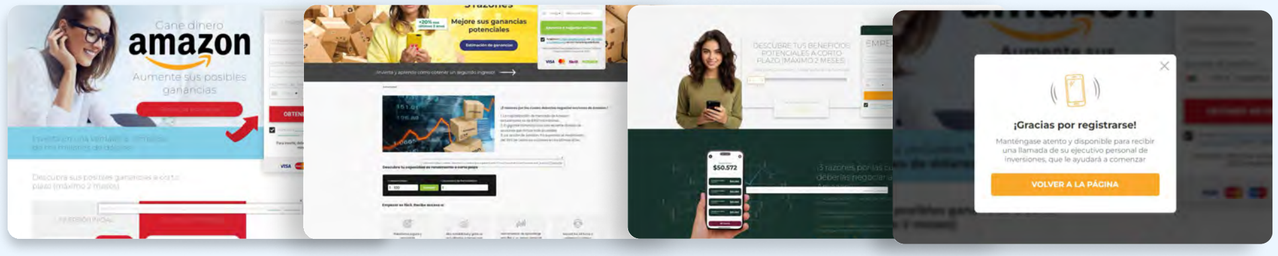


- Impersonates Microsoft, Windows, or Apple, offering fake virus protection services.
- Various attacks display a phone number, using social proof to manipulate users through social engineering
- **79% of the attacks were served in the US.**

Financial Scam

Malicious Domain:
readbuzzhub.com



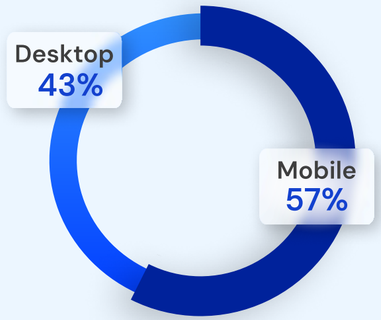


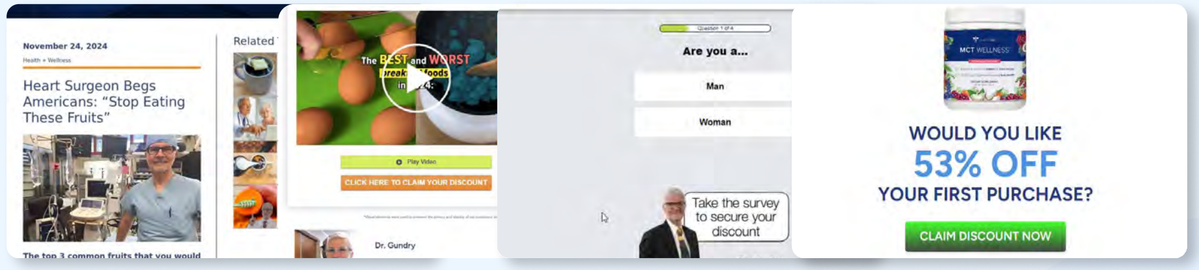
- Promotes a fake opportunity to invest in Amazon stock.
- Victims are prompted to provide their personal details. Once submitted, scammers contact victims to register them for a fraudulent trading service.
- **67% of the attacks were served in the US.**

Q4 Malvertising Clickbait Attacks
The Holiday Season's Hidden Threats

Misleading Product Offer

Malicious Domain:
thehealthiestfat.com



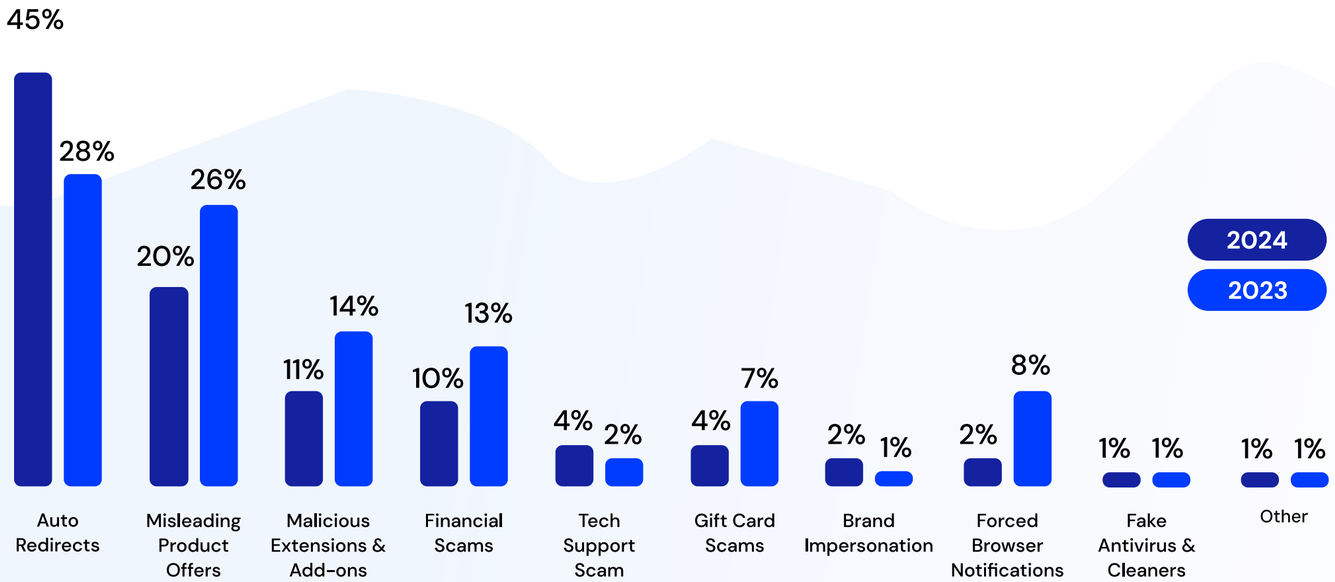


- Promotes a fraudulent "Dr. Gundry" product.
- The scam relies on fake articles, videos, user testimonials, and bogus discounts to mislead users.
- **64% of attacks were served in the US.**

75% of users express concerns about malware threats posed by online ads, while 70% call for stricter vetting to ensure ad safety.

GeoEdge User Survey December 2024*

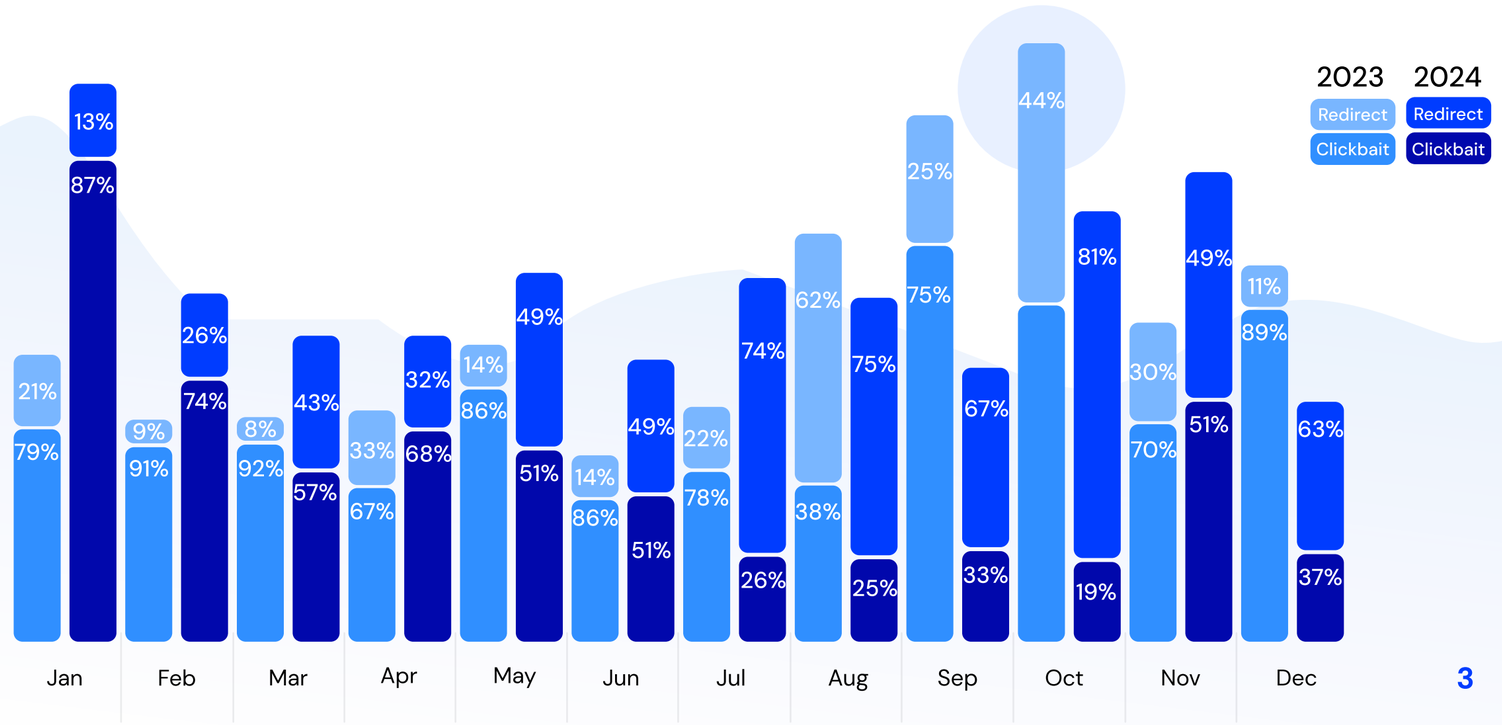
Top Malvertising Attack Vectors



In 2024, **auto-redirects accounted for 45% of all malvertising attacks, up from 28% in 2023 — a 25% increase in impressions. Misleading product offers dropped by 40%, and malicious extensions and add-ons fell by 50%, reflecting a shift in attacker tactics.** Tech support scams and brand impersonation schemes nearly doubled in volume, though their overall scale remains relatively small.

Redirects Vs Clickbait 2024 Vs 2023

Malvertising levels in 2024 rose by 10% compared to 2023, with October 2024 reaching a new peak as redirects accounted for 81% of all malicious ads — the highest level on record.

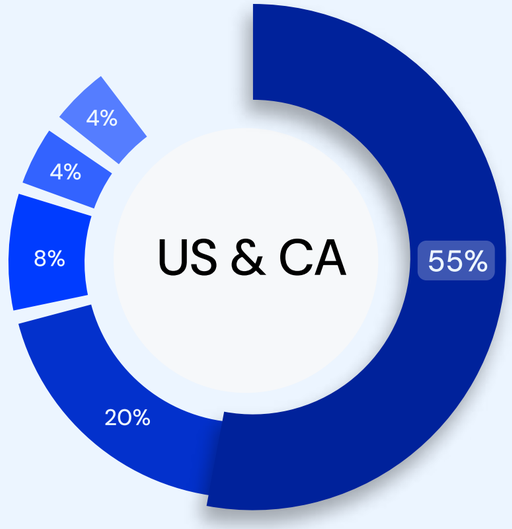


Malvertising Attacks By Region

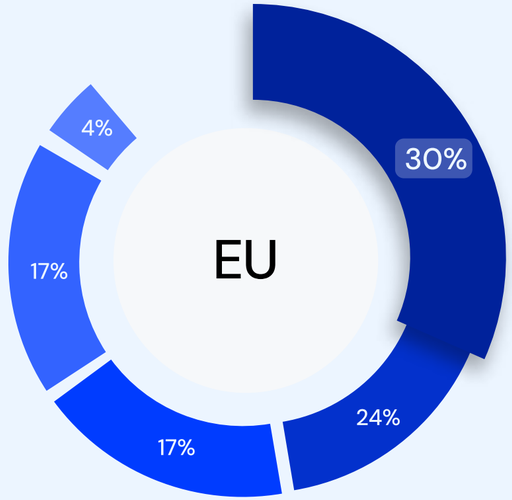
Auto-Redirects Dominate Global Malvertising Attacks

Auto-redirects dominated malvertising in the U.S. and Canada, making up 55% of all malvertising attacks in the region. In contrast, auto-redirects were less prevalent in the EU and APAC, comprising around 30% of malvertising activity.

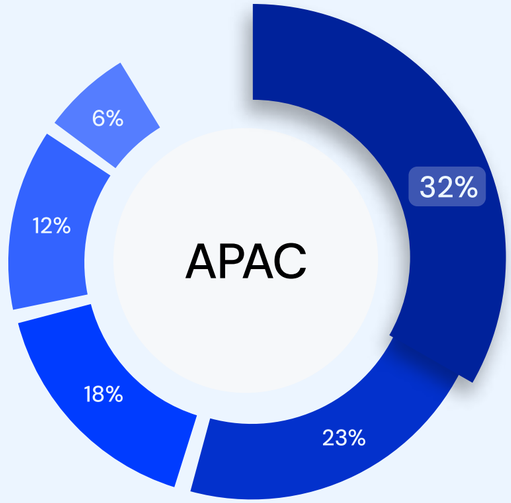
Financial clickbait scams further highlighted regional disparities. In APAC, these scams ranked as the second most common malvertising vector, making up 23% of incidents. This contrasts sharply with the U.S., where financial clickbait accounted for just 4%.



- Auto Redirect
- Misleading Product Offer
- Malicious Extensions & Add-ons
- Gift Card Scam
- Financial Scam



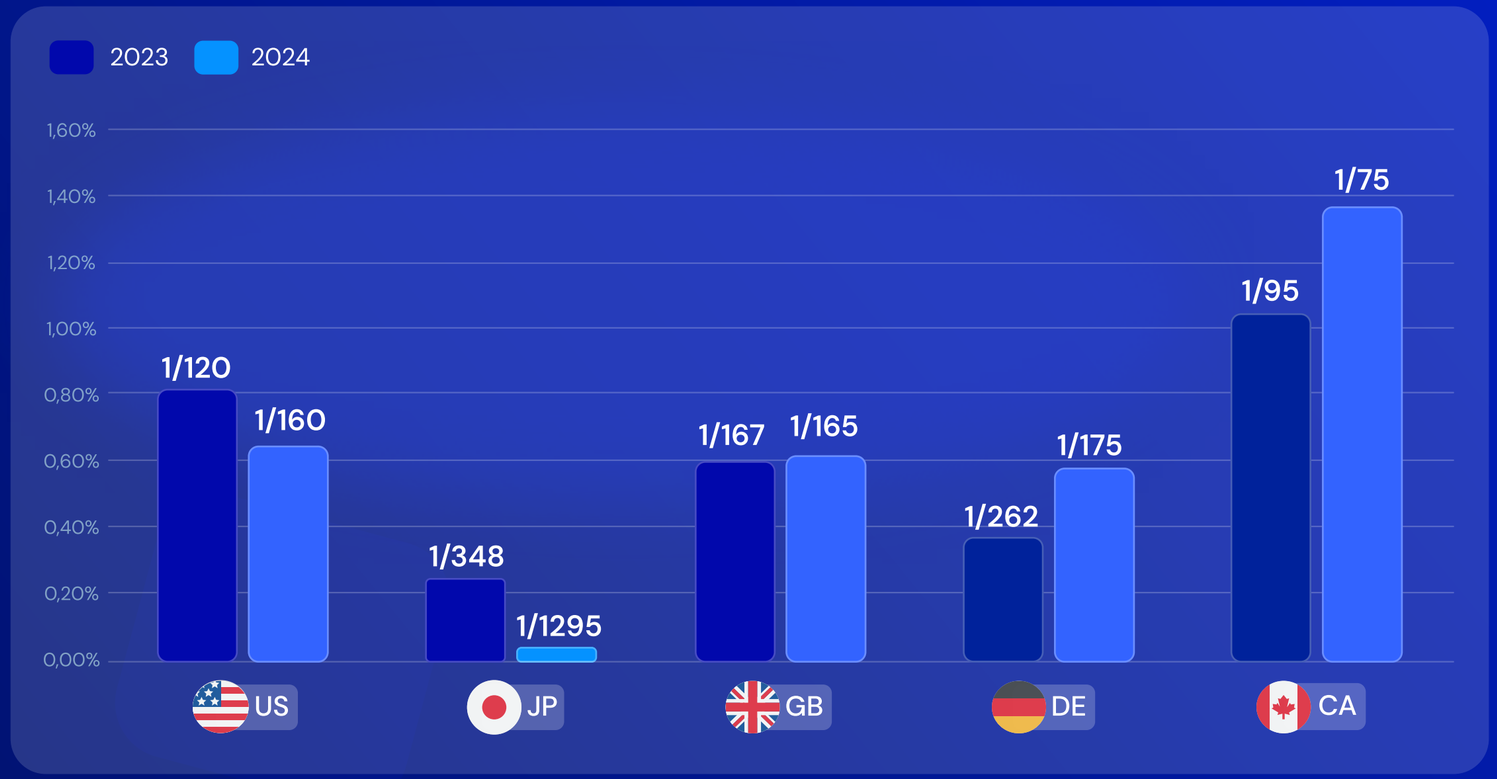
- Auto Redirect
- Misleading Product Offer
- Financial Scam
- Malicious Extensions & Add-ons
- Gift Card Scam



- Auto Redirect
- Financial Scam
- Misleading Product Offer
- Tech Support Scam
- Forced Browser Notifications

Malvertising by Region: A Global Snapshot

Auto-Redirects Lead in North America Financial Scams Dominate in APAC



**Malicious ad levels across regions tracked based on overall impressions served.*

The US malvertising rate showed a slight improvement, with malicious ads declining from 1: 120 impressions in 2023 to 1: 160 impressions.

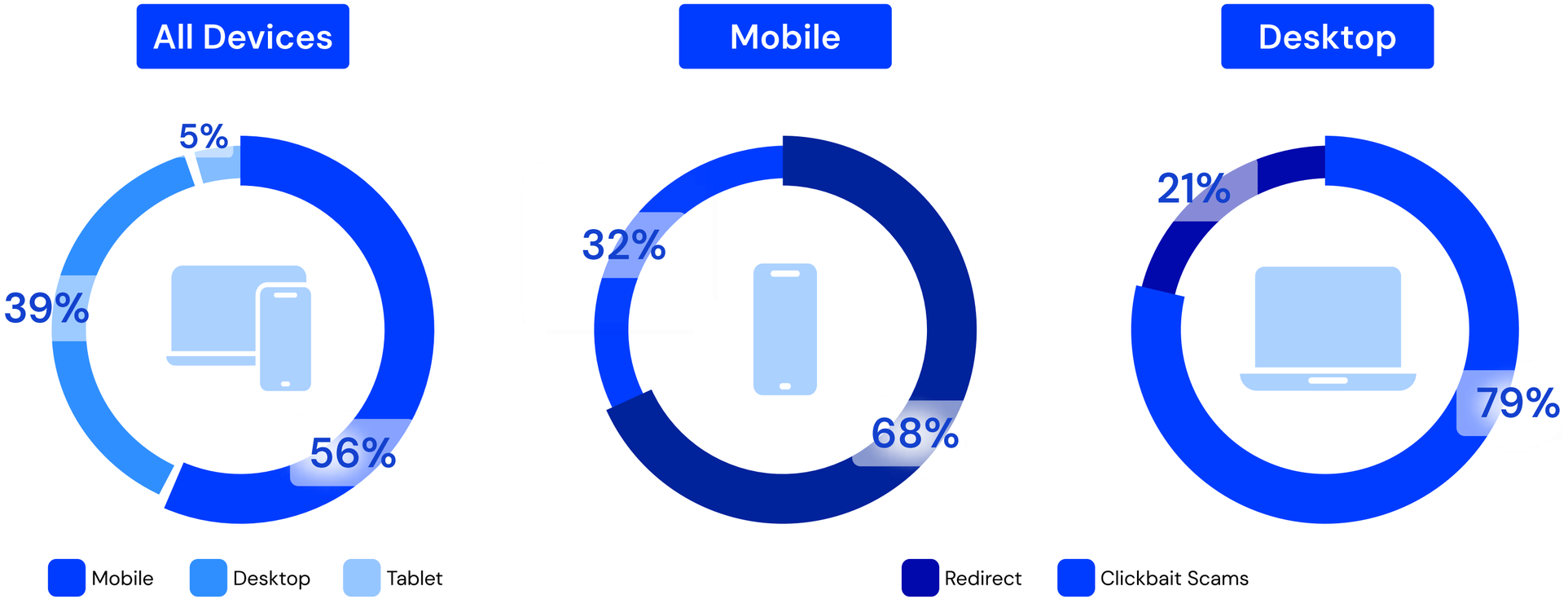
Japan demonstrated significant progress, achieving a 75% reduction in malvertising rates.

Germany experienced a 45% increase in malicious activity, with users encountering malicious ads once every 175 impressions.

Canada remained a high-risk region, with malvertising scams appearing at 1 in every 75 impressions.

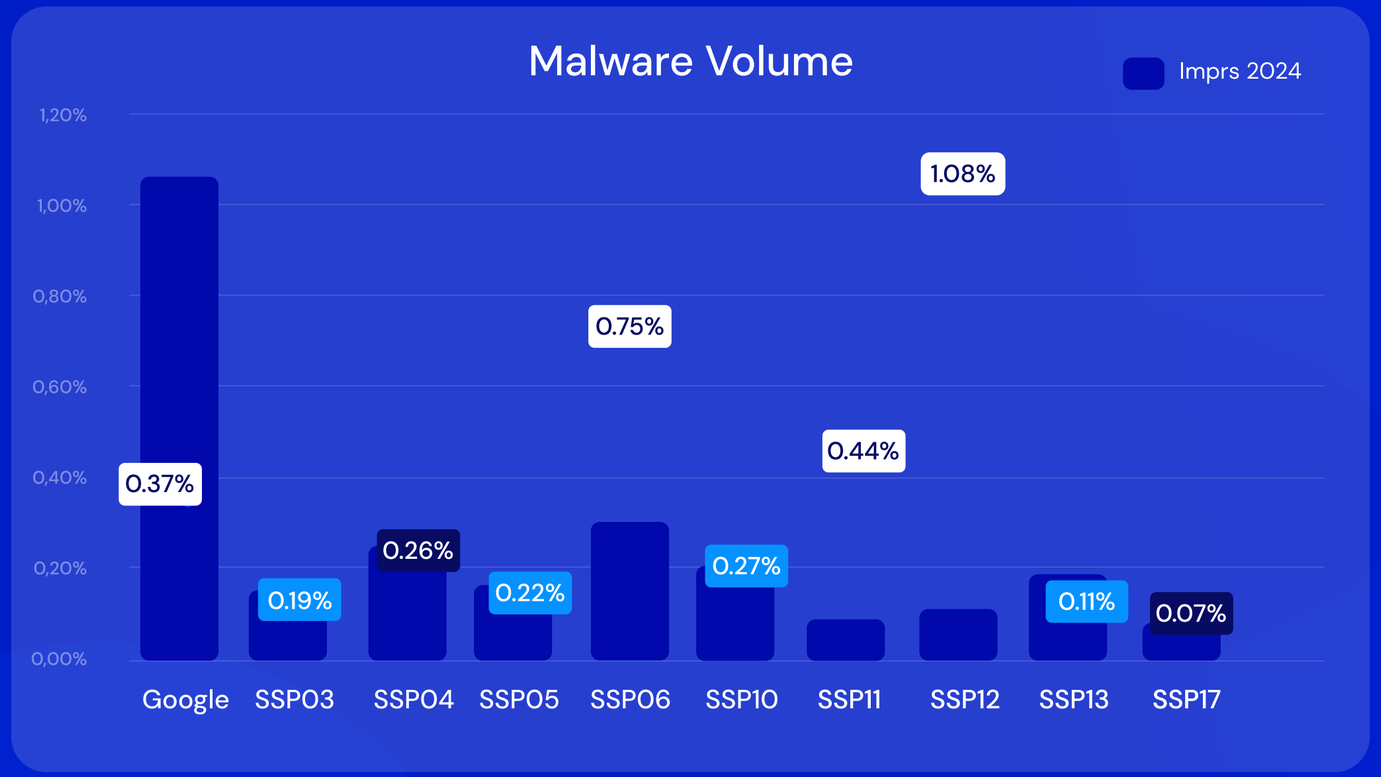
Learn More

Malvertising Across Devices



56% of malicious ads targeted mobile users. Among these, 68% were caused by redirects, while 79% of desktop attacks relied on clickbait.

Global SSP Rankings: Malvertising Rates



Improvement

- Google
- SSP06
- SSP11
- SSP12

Decline

- SSP04
- SSSP17

Underperforming Players: SSP04, the 3rd largest SSP, saw a significant increase in malvertising infection rates, exceeding 10%. SSP06, despite some improvement, still exhibits high infection rates compared to others in the top 10. SSP11 and SSP13, while improving slightly, continue to show concerning levels of infections.

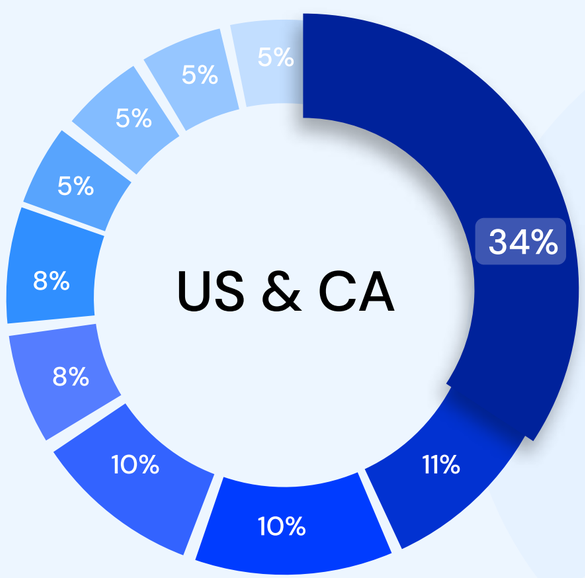
Improved Players: Google and SSP06 showed progress, though SSP06's rates remain relatively high. Smaller SSPs like SSP11 and SSP13 also saw slight improvements but still reported elevated infection levels.

Learn More

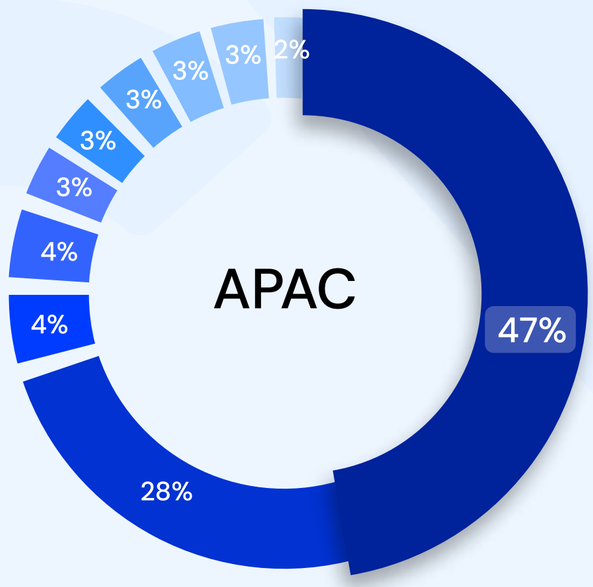
Ad Content Blocked By Region

Gambling ads dominate filtering globally, with the EU seeing the highest share at 69%, compared to 47% in APAC and 34% in the US & CA. The US & CA have more diverse filtering priorities, with significant shares in marijuana, weapons, and politics.

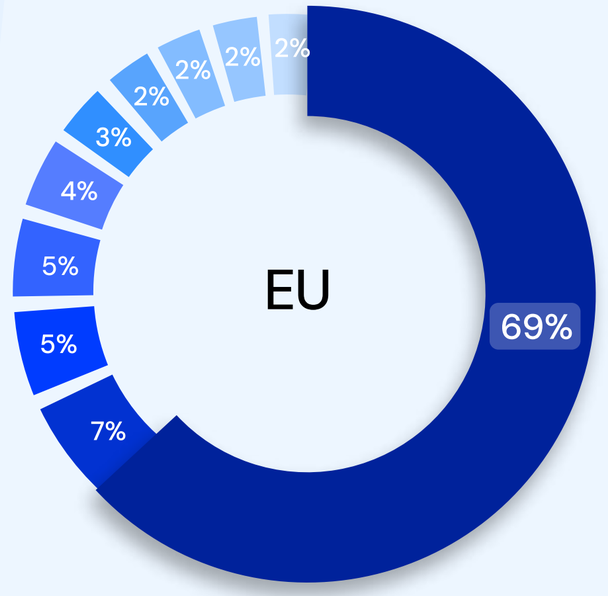
APAC stands out with a notable 28% in pharmaceutical-related ads, reflecting regional regulatory challenges. Weight loss ads are emerging as a concern in both the EU (7%) and US & CA (5%).



- Gambling
- Weapons
- Tobacco
- Law, Government & Politics
- Election
- Marijuana
- App Store Category - Games
- Weight Loss
- Alcohol
- News and Media



- Gambling
- Tobacco
- Pharmaceuticals
- App Store Category - Games
- Weapons
- Swimwear and Intimate Apparel
- Law, Government & Politics
- Cryptocurrency
- Religion
- News and Media



- Gambling
- Swimwear and Intimate Apparel
- Health
- Law, Government & Politics
- Tobacco
- Weight Loss
- News and Media
- Weapons
- Alcohol
- Marijuana

Ensure User Protection and Quality Ad Experiences with GeoEdge

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