Adsterra Malware Zero-Tolerance Policy: What You Need to Know

1. Introduction

Being the legitimate advertising and monetization platform, Adsterra prohibits malvertising and scam methods down to a complete and irrevocable ban of those advertisers and publishers whose practices are proved to be illegal or, by any means, abusive to Adsterra and its partners.

In tandem with our Policy Team, we have prepared an introduction to the Adsterra Malware Zero-Tolerance Policy that states the following:

- ➔ Adsterra does not serve malware intentionally or willingly;
- ➔ Our security systems provide 360-degree malware protection;
- ➔ Adsterra does not intentionally work with offenders or profit from their activities;
- ➔ Official Terms and Conditions prohibit any malicious activities within or by the medium of Adsterra.

To deliver you a clear picture of why any former or possible malware allegations are baseless, we will introduce how the ad network works and how it protects its partners, including prevention and combat techniques.

2. Why any Adsterra malware intentional spreading allegation is groundless

We assume that some accusations could appear as an outcome of shallow knowledge about how the ad network operates. Adsterra is a technological platform that multiple users can access. It has been one of the most used advertising and monetization platforms since 2013, serving over 20K ad campaigns simultaneously.

Adsterra brings together two groups of actors: advertisers (aka advert suppliers) and publishers (aka website owners, webmasters) who exchange valuable content. It only means that the ad network itself does not produce any content that could be considered good or bad. It only provides algorithms to serve traffic and ads.

Like any other software accumulating numerous user accounts, Adsterra can be attacked by hackers or violators aiming at spreading malicious programs and viruses by its means. But it can be neither a direct undertaker of such activities nor a beneficiary of those. In contrast, the Ad Network constantly prevents attempts to disrupt its users and their traffic sources.

3. When tech platforms like Adsterra may be suspected of spreading malware intentionally

As said earlier, ad networks bring together two groups of users: advertisers and publishers. Most of them provide self-service platforms for advertising and monetizing, which allows for placing advertising and adding traffic sources.

Any advertising or tech platform network may fall under the attack of unprincipled organizations and individuals whose aim is to disrupt as many traffic sources as possible. They deliberately insert malicious scripts inside landing pages, creatives, and URLs disguised as whitehat advertising. When not detected by security systems, these scripts can become a part of a regular ad feed on publishers' websites.
End users come across rip-off techniques when visiting publishers' websites with advertising.

Eventually, an ad network that was not involved in producing malware could become a means of its delivery. Taking into account all possible repercussions, including tangible financial and reputational losses, one can be sure that **ad networks are not by any means interested in spreading malware and fraudulent content.**

All mentioned above does not mean that advertising networks are not obliged to undertake decisive measures to prevent and combat attempts to malvertise on their premises.

Being a widespread self-service platform with a strong reputation, Adsterra has never denied its duty to take care of partners. Moreover, we are developing a highly secure, relatively impenetrable ecosystem for running ad campaigns and monetizing inventory.

Along with anti-malware measures, Adsterra is constantly enhancing its premises protection, which implies:

- ➔ Servers, data centers, and infrastructure security
- ➔ SSL data transmission
- ➔ Payment security
- ➔ Encryption of all communications, etc.

4. How Adsterra malware protection works ensuring the highest level of security

Just like other tech and software giants whose platforms and services are widely used by thousands of individuals and businesses, Adsterra implements a set of robust measures to discover ad fraud and malware before it affects the network's users.

Since 2013, malware detection at Adsterra has come a long way in developing its in-house safety instruments and adapting the most effective third-party technologies.

Today, we provide our partners with state-of-the-art automatic protection paired with manual checking of advertising feed performed by the in-house Policy Team.

4.1 The 3-level-security system for Adsterra advertisers and publishers

4.1.1. Automatic prevention and blocking of malware threats
Adsterra has continually been investing in superior safety algorithms, both in-house and provided by reputable third parties. Apart from the widely-used GeoEdge, we put in force highly accurate in-house techniques designed completely to adapt the mechanics of serving advertisements and traffic.

Adsterra effectively prevents and blocks malware and undesirable software programs (such as viruses, trojans, etc.), ensuring traffic sources registered on our platform are clean from malicious codes and safe to end-users.

We take care of each advertiser and publisher, consistently training our algorithms to detect and block the newly-appearing cyber threats in malvertising.

4.1.2. Manual checking of traffic and ad feed
Along with automated systems and algorithms, Adsterra holds its Policy Team. These highly experienced experts implement security improvements, train AI algorithms to combat the most advanced cyber threats, carry on in-depth research of new threats, and monitor ad feed manually.

Policy Team can manually ban suspicious tracking links, landing URLs, as well as block the whole ad campaigns and accounts.

4.1.3. Prompt response to tickets and inquiries regarding malware on Adsterra advertising network
Staying in contact with all our partners has always been one of the top Adsterra's priorities. All advertisers and publishers, as well as any individual or legal entity coming across with our ads have several channels to report suspicious activities and questionable advertisements looking forward to Adsterra reacting as quickly as possible.

While Adsterra partners mostly use in-platform communication options, any other Internet user can report abuse via the form on adsterra.com.

When receiving a complaint, Adsterra will launch an investigation that implies: automated scanning and manual expert check. The suspected actor must prove and warrant that their advertising or web traffic is malware-cleaned and secured.

The Adsterra Policy Team will suspend and block all suspicious accounts until the investigation is over and their activities are proved warrantable.

5. Adsterra Terms & Conditions prohibit malware and fraud traffic

Apart from enforcing the superior anti-malware and anti-cheat solutions, Adsterra initially prohibits any unlawful activities asking its partners to agree to Terms and Conditions before registering on the platform.

All Adsterra's advertisers and publishers need to agree to those Terms and Conditions to start using Adsterra services. Terms for advertisers and Terms for publishers state that we prohibit any malicious practices aimed at attacking users' software program or inventory, privacy breaches, any types of phishing, adware, trojans, viruses, spoofing, and other offensive actions.

Any attempt of unlawful and abusive advertising, as well as streaming fraudulent traffic, will be banned down to the full and irrevocable.
Therefore, all allegations regarding Adsterra's intentional cooperation with offenders are false.

Terms and conditions - Advertisers
Terms and conditions - Publishers

6. Main points about possible former and future Adsterra malware allegations

As stated above, Adsterra has in no way been producing or endorsing malicious advertisements and traffic.

#1. Adsterra Ad Network claims all allegations mentioning it is deliberately associated with malware spreading or cooperation with unlawful entities to be false and groundless.

#2. Moreover, as one of the market-leading ad-tech players, Adsterra is continually preventing and combating malvertising. The Ad Network has been developing its in-house security algorithms. The Adsterra Policy Team takes control over the whole ad feed and all traffic sources.

#3. All of Adsterra's partners have to agree to Terms and Conditions, which demand serving only safe and clean advertising materials: URLs, landing pages, pre-landers, creatives, etc.

#4. Every Adsterra partner has full access to our support team and can report any suspicious activity, being sure to get the quickest resolution.

#5. Any Internet user is free to report abuse or violation of our Terms and Conditions from the website adsterra.com (link in the footer part).

7. Conclusion

Thank you for sharing your time with this official Adsterra Malware Statements. We respect that you are involved in the topic and can guarantee that in Adsterra, you have observed a dependable and caring partner.