Online Trust Alliance

# Malicious Ads & Content Response & Remediation Guide

**Overview**
The Response and Remediation Guide is one of a series of best practices that OTA has published to help protect businesses and to respond effectively to the threat landscape and online fraud battlefield. One of the ways in which malware perpetrators attempt to infiltrate online advertising and content publishing networks is by creating fraudulent advertisers or advertising agencies that appear to represent legitimate brands. The frequency of malicious advertising insertions continues to grow with increased precision and payload capabilities.

The following guidelines have been developed to aid the advertising and marketing communities in effectively preparing for and responding to malvertising and related incidents.

---

**1. Organize a Response Team**
Form and train a dedicated team to oversee responsibility for the problem. Team members should act as in-house subject matter experts on threats and vulnerabilities, and provide guidance to management team about risks in the advertising landscape.

**2. Create a Communication Plan**
Create an internal communication piece to educate other employees about the problem. Help other employees understand how to handle a “bad ad” when witnessed in the wild. Let others know what information is helpful for the response team (screenshots, call flows, etc.) Encourage the use of tools such as AdMagic, Ghostery and AdChoices to help identify ad sources.

**3. Understand Different Complaint Types**
Identify and define the different complaint types and create a response plan for each type. For example, handling a viewer complaint about a pop-up ad will require a different set of steps than handling a complaint about a fake anti-virus ad. Understanding the different complaint categories will also help provide metrics to management.

**4. Gain Agreement on Immediate Steps**
Predefine immediate steps and gather buy in from affected parties *before* an incident takes place, as making decisions under pressure can cause unwarranted stress and delays. Considerations:

- Shut off all advertising?
- Shut off only ad network advertising?
- Run house ads only?
- Run tests in a test environment?
- Other?

**5. Ongoing Scanning and Screening**
Scan all tags regularly using a tag or site screening system. While no system can guarantee the safety of every single ad impression when served by a third party, they can provide peace of mind to the team that there is at least some visibility to the ad traffic.

 

**6. Gather Emergency Contact Information during Onboarding Process**
Allow only authorized ad networks and providers to run on your site. Gather emergency contact names and phone numbers to use when a questionable ad appears on your site. Work with the ad networks to understand their own remediation plan when a problem occurs. Be sure that to record and document network violations for malvertising. Determine if your organization should set up a "three strikes" policy or some other penalties for repeated problems.

**7. Create an Incident Response Plan & Communication Plan**
As malvertising, data loss incidents and breaches are an increasing occurrence targeting the ad supply chain and interactive marketers, the creation and testing of a response plan is key. All businesses need to proactively develop a plan to minimize data collection, enhance data protection and to create a customer-centric incident response plan. A key component of a plan is setting up emergency contact notification templates to help communicate to your business partners and customers. Defining a process, call tree and team responsibilities in advance, can help minimize partner issues and the business impact resulting from malvertising and related incidents. By planning, businesses of all sizes can minimize their risks, costs and the impact.

For more information see 2013 OTA Data Protection & Incident Readiness Guide.
https://otalliance.org/breach.html

For related resources and updates to this document visit https://otalliance.org/3PIntegrity.html
Send comments and suggestions to admin @ otalliance.org.

**About The Online Trust Alliance (OTA) https://www.otalliance.org/**
OTA is an independent non-profit with a mission to develop and advocate best practices and public policies which mitigate emerging privacy, identity and security threats to online services, organizations and consumers, thereby enhancing online trust and confidence. By facilitating an open dialog with industry, business and governmental agencies to work collaboratively, OTA is making progress to address various forms of online abuse, threats and practices that threaten to undermine online trust and the vitality of online services and commerce.



Revised 4/3/2014