



Timeline of a **Malvertising Attack**

How malicious ads go from idea to threat and how HUMAN Malvertising Defense helps publishers protect their valuable revenue from this ever-evolving threat.

Malvertising threats for Publishers



Redirects away from publisher sites



Ad cloaking to execute clickbait scams



Redirects to malicious landing pages



Distribution of malware



Client-side injections to steal user info



Heavy ads slowing site experience



Pixel/Video Stuffing



Bad actor creates malicious code and sets up a programmatic ad campaign





Bad actor submits their campaign for creative review



Pre-scanning tools check for malicious activity in creative, but malvertiser evades blocklist detection



4



Bad actor's campaign wins auction bid

Without HUMAN



Blocklists try to catch known bad actors, but malvertiser evades blocklist detection



Creative renders and malvertiser pays for impressions



Code begins to execute malicious activity



Malicious activity affects users and damages publisher revenue

Solutions Fall Short

Where Blocklist





Non-malicious ads can get blocked, causing unwanted revenue loss

Add Latency



Size of the blocklist can cause latency on pages due to list load

Easy to Evade



Blocklists are reactive and only as good as the entries within them.

Put Revenue at risk



Blocking ads and requesting new creative can risk revenue or diminish user experience

Protected by HUMAN Malvertising Defense





Malvertising Defense scans all creatives on page and analyzes landing pages to detect malicious behavior





Creative renders, but malicious behavior is blocked







Malicious code never executes. User never lands on "Congrats" page





User experience is unaffected, publisher revenue is protected and malvertiser will look elsewhere for future attacks



Malvertising Defense Advantage



Preserve Revenue



Protect Brand Reputation



Optimize Performance and Overhead

Take Control of Your Digital Ad Inventory