
seven.one
ENTERTAINMENT
GROUP
AD FRAUD

1. ÜBERBLICK: AD-FRAUD-ARTEN UND –TECHNIKEN

Ad Fraud
ist die betrügerische Erzeugung von Online-Werbung, Klicks, Conversions oder anderer Ereignisse, um ungerechtfertigte Einnahmen zu erzielen.

Ad Fraud-Arten	Ad Fraud-Techniken		
Fake Traffic ist Traffic, der mit dem Ziel generiert wird, Impressions oder Klicks zu erhöhen; er kann von echten Nutzern oder von Bots generiert werden.	Ad Stacking	Pixel Stuffing	Click Fraud / Impression Fraud
Fake Placements sind unzulässige Online Ads, die authentische Schaltungen vortäuschen.	Domain Spoofing	Ad Injection	Geo Masking / Location Fraud
Fake Actions sind Techniken, die tatsächliches Nutzerverhalten vortäuschen.	Affiliate fraud	Retargeting fraud	Conversion fraud

Quelle: P7S1 Market Intelligence, Definition from Oracle; Journal of Cybersecurity and Privacy: “Ads and Fraud: A Comprehensive Survey of Fraud in Online Advertising (Dec 2021); Springer “Fraud Prevention in Online Digital Advertising”(2017)

2. AD FRAUD: VERLUSTE UND SCHÄDEN AUF MEHREREN EBENEN

$68 Mrd.

Direkt durch Ad Fraud verursachte Schäden für Werbekunden und Publisher

Der finanzielle Gesamtschaden für Werbetreibende und Publisher ist schwer zu beziffern, da einige Ad Fraud-Aktivitäten unbemerkt bleiben. Aktuelle Schätzungen veranschlagen den Schaden auf **weltweit 68 Mrd. $[1], wovon ca. 2 % auf Deutschland entfallen.[2]**

Folgeschäden für Unternehmen sowie die gesamte Branche

Der Schaden durch Folgewirkungen dürfte noch einmal doppelt so hoch sein. So treffen Unternehmen etwa auf Grundlage von Ad Fraud-belasteten Kampagnenergebnissen falsche Entscheidungen. Außerdem müssen Unternehmen Ressourcen für die Vermeidung von Ad Fraud aufwenden.

Weiterer Schaden für Gesellschaft und Umwelt durch die mit Ad Fraud verbundene Schattenwirtschaft

Weitere Auswirkungen von AdFraud sind Verschwendung von Ressourcen, Klick-Farmen mit problematischen Arbeitsbedingungen, Förderung von Fake News sowie ökologische Schäden (siehe Kasten Co2-Fußabdruck). **Der finanzielle Schaden beträgt vermutlich ein Vielfaches des direkten Schadens.**

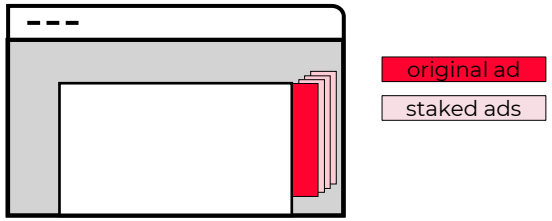
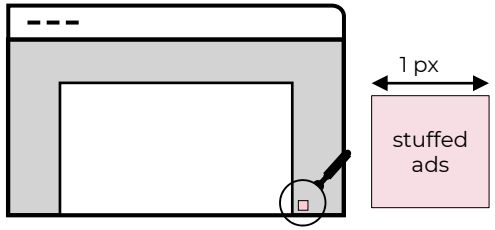
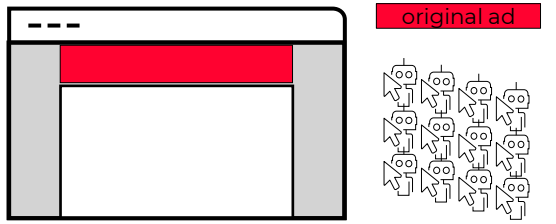
CO2-FUßABDRUCK VON AD FRAUD:

- Online-Werbung verursacht CO2-Ausstoß durch Produktion der Werbemittel, Auslieferung der Ads, Anzeige der Ads auf den Devices der Nutzer sowie Messung/Validierung der Kampagnenleistung.
- Ad Fraud verursacht einen relevanten Teil der CO2-Emissionen und hat im Gegensatz zu legitimer Werbung keine positiven Effekte.
- Darüber hinaus kann Ad Fraud mehr Energie verbrauchen als normale Werbung, z. B. wenn Websites aufgrund von Ad Fraud langsamer laden, was zu einem höheren Energieverbrauch führt.
- Der gesamte CO2-Ausstoß von Ad Fraud könnte bis zu 14 Millionen Tonnen pro Jahr betragen[3]. Dies entspricht dem Energieverbrauch von 1,5 Millionen Haushalten in einem Jahr [4].

seven.one ENTERTAINMENT GROUP

Quelle: P7S1 Market Intelligence, Cheq: “The impact of invalid traffic on marketing”
1) Juniper Research (Feb 2022); 2) Cheq.ai (Jan 2021); 3) Environmental impact assessment of online advertising, Pärssinnen, Kotila, Cuevas, et al., 2018;
4) https://www.epa.gov/energy/greenhouse-gas-equivalencies-calculator

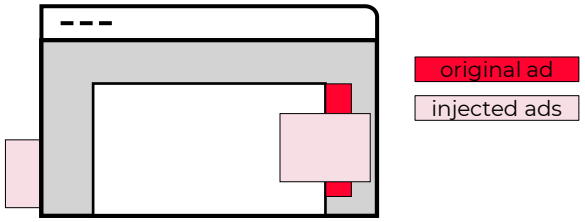
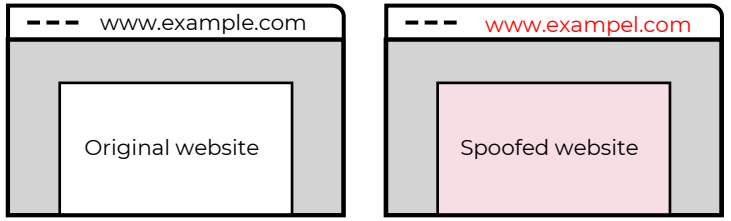
3. AD-FRAUD-ARTEN (1/3): FAKE TRAFFIC (NICHT GESEHENE ADS)

	Ad Stacking Eine echte Ad Impression, mehrere gefakte Ad Impressions	**Pixel Stuffing** Nicht sichtbare, in ein Pixel gequetschte Ads	**Click Fraud / Impression Fraud** Von gefakten/unechten Nutzern erzeugte Impressions oder Klicks
Beschreibung	Unter Ad Stacking versteht man die Schichtung von Ads in einer einzigen Ausspielung, so dass nur die oberste Werbung sichtbar ist. Alle Ads im Stapel werden jedoch für jede Impression/jeden Klick gezählt. 	Eine oder mehrere Ads oder ganze Websites werden in einem Pixel platziert, das mit dem bloßen Auge nicht erkennbar ist. Obwohl die Nutzer dies nicht bemerken, „sehen“ sie mehrere Ads, sobald die Seite geladen ist. 	Bots oder menschliche Klick-Farmen sehen oder klicken auf Werbeeinblendungen, wodurch Ad Impressions und Klicks in die Höhe getrieben werden, obwohl es keine echten Nutzer gab. 
Schaden	Nur die oberste Werbung wird gesehen, aber den Werbekunden werden auch die gefakten Ad Impressions in Rechnung gestellt. Zudem erzeugen von Ad Stacking betroffene Kampagnen verzerrte Reportings, die sich auf die weitere Werbestrategie auswirken können.	Den Werbekunden werden Anzeigen in Rechnung gestellt, die von den Nutzern nicht wahrgenommen werden. Impressions, die durch Pixel Stuffing erzeugt werden, können nicht zu Conversions führen. Wie beim Ad Stacking erzielen die betroffenen Kampagnen verzerrte Ergebnisse.	Werbetreibende bezahlen für gefälschte Impressions / gefälschte Klicks. Erhöhter Web-Traffic verursacht längere Ladezeiten der Websites und Energieverschwendung. Erzeugung verzerrter Kampagnendaten (Ad Impressions, Click-Through-Rate, Cost-per-Click).
Fußabdruck & Begrenzung	Ad Stacking ist eine der häufigsten Formen des Ad Frauds und verursacht ca. 20 % der weltweiten Werbeausgaben.[1)] Obwohl Ad Stacking häufig vorkommt, ist es relativ einfach zu erkennen und es gibt Methoden, mit denen Ad Stacking verhindert werden kann. Werbekunden können auch eigenhändig ihre Reportings überprüfen und Auffälligkeiten erkennen, z. B. niedrige CTRs.	Pixel Stuffing ist eine der einfachsten Ad Fraud-Arten für Cyber-Kriminelle, aber Ad-Fraud-Detection-Technologien erkennen Pixel Stuffing. Da diese Art von Ein-Pixel-Werbemittel keine Wirkung erzielen kann, ist die beste Möglichkeit, Pixel Stuffing zu verhindern, die Abkehr von CPM-Modellen (also von rein auf Impressions basierenden Abrechnungsmodellen).	Click Fraud ist eine sehr häufig auftretende Form des Ad Frauds. Sie erfolgt in der Regel in großem Umfang – Betrüger verwenden Bots, die immer wieder "klicken". Solche Bot-Aktivitäten können bis zu einem Drittel des Website-Traffics ausmachen.[2)] Click Fraud kann durch den Vergleich von CPM, CPC und CTR auf verschiedenen Plattformen erkannt und durch Cost-per-Action-Modelle vermieden werden.

seven.one ENTERTAINMENT GROUP

Quelle: 1) fraudblocker.com 2) Imperva, Bad Bot Report, 2022;
Journal of Cybersecurity and Privacy: “Ads and Fraud: A Comprehensive Survey of Fraud in Online Advertising (Dec 2021);
Springer “Fraud Prevention in Online Digital Advertising”(2017)

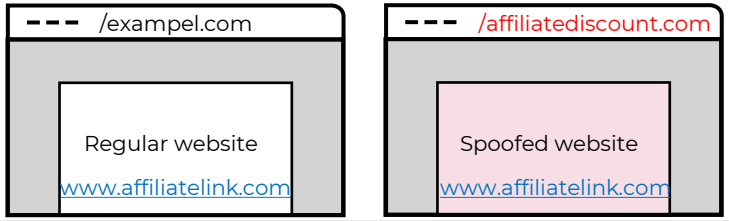
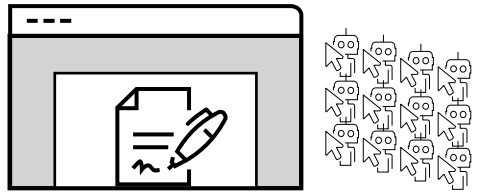
3. AD-FRAUD-ARTEN (2/3): FAKE PLACEMENT (BETRÜGERISCH PLATZIERTE ADS)

	Ad Injection Ads auf unzulässigen Platzierungen	**Geo Masking** Manipulierte Standortdaten	**Domain Spoofing** Gefälschte Websites geben vor, seriös zu sein
Beschreibung	Ad Injection platziert Werbung mit einer Software an einer Stelle auf der Website, an der sie nicht sein sollte. Entweder werden neue Ads an beliebiger Stelle eingefügt oder bestehende Ads werden ersetzt.  	Geo-Masking kapitalisiert die Tatsache, dass Traffic aus einer Region wertvoller sein kann als aus einer anderen. Betrüger nutzen Geo-Masking, um minderwertigen Traffic zu verschleiern und Werbenden vorzutäuschen, es handele sich um höherwertigen Traffic aus einer begehrten Region.  	Cyber-Kriminelle erstellen gefälschte Webadressen, die legitime Websites imitieren, und versuchen, Nutzer auf diese Seiten zu locken oder von Tippfehlern zu profitieren (Typo Squatting). 
Schaden	Ad Injection findet in verschiedenen Formen statt: Ads werden über reguläre Platzierungen gelegt oder ersetzen andere Ads vollständig, sodass diese nicht mehr zu sehen sind. Die Ads können Inhalt verdecken und die Usability der Website beeinträchtigen. Ad Injection kommt oft in Kombination mit bösartiger Software vor, um legitime Klicks abzuschöpfen.	Werbetreibende zahlen höhere Preise für das Targeting bestimmter Standorte. Mit Geo Masking werden Werbebudgets, die für das Geo Targeting eingesetzt werden, verschwendet. Geo Masking verringert auch die Effektivität der Kampagne und führt zu verzerrten Kampagnenergebnissen, wenn Werbung an falschen Standorten ausgeliefert wird.	Fake Websites werden zu Premium-Preisen verkauft, bieten aber keine Premium-Inhalte. Domain Spoofing wird auch für Phishing oder Scamming eingesetzt. Dabei wird versucht, die Opfer dazu zu bringen, auf bösartige Links zu klicken oder persönliche Daten preiszugeben. Betroffene Unternehmen riskieren eine Rufschädigung.
Fußabdruck & Begrenzung	Ad Injection verbreitete sich in den frühen 2010er Jahren, als moderne Browser die Installation von Erweiterungen und Symbolleisten ermöglichten. Freeware und vorinstallierte Software enthielten oft Ad Injectors. Heute spielt Ad Injection nur noch eine untergeordnete Rolle, da die meisten Browser und Virenprogramme verhindern, dass die Malware funktioniert. Dennoch gibt es nach wie vor Kampagnen wie die bekannte "Ihr Computer ist infiziert„-Anzeige.	Aktuelle Studien zeigen, dass Geo-Masking eine weit verbreitete Technik des Ad Frauds ist, insbesondere auf mobilen Geräten, wo Apps jeden beliebigen Standort in einer Auslieferungsanfrage weitergeben können. Auch kostenlose VPN-Dienste und der IP-Service Private Relay von Apple sind Einfallstore für Geo Masking. Werbekunden können den Betrug verhindern, indem sie sich auf zusätzliche Identifikatoren verlassen oder Datenverkehr über VPN-Dienste ganz ausschließen.	Domain Spoofing erfolgt oft in Kombination mit Email Spoofing und einige große E-Commerce Unternehmen und deren Kunden wurden bereits Opfer. Die einfachste Möglichkeit, Spoofing zu verhindern, besteht für die Nutzer darin, sensibel für Phishing-Mails zu sein. Unternehmen können Beschwerden bei der ICANN einreichen, Google gefälschte Websites melden und ähnlich aussehende URLs registrieren lassen.

seven.one ENTERTAINMENT GROUP

Quelle: Journal of Cybersecurity and Privacy: “Ads and Fraud: A Comprehensive Survey of Fraud in Online Advertising (Dec 2021); Springer “Fraud Prevention in Online Digital Advertising”(2017)

3. AD-FRAUD-ARTEN (3/3): FAKE ACTIONS (VORGETÄUSCHTES NUTZERVERHALTEN)

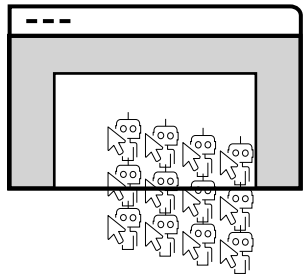
	Affiliate Fraud Unseriöse Gewinnung von Affiliate Provision	**Retargeting Fraud** Gefälschte Nutzer, die vorgeben, Nutzer zu sein, die es wert sind, erneut angesprochen zu werden	**Conversion Fraud** Gefälschte Conversions
Beschreibung	In einem Affiliate-Netzwerk erhalten Partner, die User über Links auf ihrer Website auf die Website eines anderen bringen, eine Provision. Affiliate-Betrug ist, wenn User mit betrügerischen Techniken auf die Website des Affiliates gebracht werden. 	Dem Werbekunden wird vorgetäuscht, dass die Fake User (z.B. Bots) potenzielle Käufer sind, die per Retargeting angesprochen werden sollten. **Regular Retargeting:** Identifikation interessanter Nutzer auf Basis bisheriger Web-Aktionen (über Drittanbieter-Cookies)  **Retargeting Fraud:** Bots, die Web-Aktionen ausführen und Cookies erzeugen, um sich als wertvolle Nutzer auszugeben 	Um Kauf, Registrierung oder Download abzuschließen, muss der Nutzer in der Regel ein Formular mit persönlichen Daten ausfüllen. Conversion Fraud kann durch Bots oder menschliche Farmen erfolgen, die gefälschte oder gestohlene Kundendaten angeben. 
Schaden	Für Affiliate-Betrug werden verschiedene Techniken verwendet, z.B. Malware/Adware, Cookie Stuffing und URL Hijacking. Die Provision muss gezahlt werden, obwohl betrügerische Techniken verwendet wurden. Es werden verzerrte Kampagnenergebnisse mit großem Einfluss auf die Werbestrategie (Cost-per-Action-Werbung) erzeugt.	Werbetreibende zahlen einen höheren Preis für Impressions dieser gefälschten Nutzer, weil sie anhand ihres Verhaltens für interessante Kunden gehalten werden. Dies führt zu verzerrten Kampagnenergebnissen und kann die Retargeting-Strategie verfälschen.	Werbekunden zahlen einen höheren Preis für Websites mit hoher Conversion und die Website erhält ein besseres Ranking, obwohl die Rate durch Fraud erhöht wurde. Außerdem werden durch gestohlene oder falsche Kundendaten Schäden verursacht werden. Erzeugt verzerrte Kampagnendaten mit hohem Einfluss auf die Strategie (Cost-per-Action-Werbung).
Fußabdruck & Begrenzung	Große Affiliate-Netzwerke sind einem höheren Betrugsrisiko ausgesetzt als interne Affiliate-Programme. Affiliate-Betrug kann durch den Vergleich der Kampagnen-KPIs aller Affiliates identifiziert werden. So sollten beispielsweise Affiliates mit deutlich höheren Conversion Rates genau beobachtet werden.	Wenn Retargeting-Strategien nicht zu der zu erwartenden Anzahl von Conversions führen, sollte Retargeting Fraud in Betracht gezogen werden. Bot-Verkehr kann durch gängige Analyse-Tools und Validierungsdienste identifiziert werden, aber fortgeschrittene Bots sind selbst durch ausgefeilte Erkennungsmethoden schwer zu entdecken.	Conversion Fraud wird häufig für einfache Arten von Conversions wie Registrierung mit Benutzernamen oder Download einer Datei verwendet. Käufe sind nur selten das Ziel von Conversion Fraud, da sie komplexe Interaktionen und Finanztransaktionen erfordern. Erkennung von atypischem Nutzerverhalten (z.B. keine App-Nutzung nach dem Download) ist eine gängige Methode zur Identifizierung von Conversion Fraud.

seven.one ENTERTAINMENT GROUP

Quelle: Journal of Cybersecurity and Privacy: “Ads and Fraud: A Comprehensive Survey of Fraud in Online Advertising (Dec 2021); Springer “Fraud Prevention in Online Digital Advertising”(2017)

4. BOT TRAFFIC UND MENSCHLICHE KLICK-FARMEN

Bot Traffic

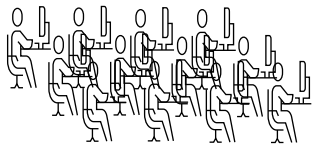


Bots sind kleine Programme oder Skripte, die einfache und sich wiederholende Aufgaben auf Websites ausführen, wie das Laden und Aktualisieren oder das Klicken von Werbung. In einigen Fällen übernehmen Bots Aufgaben wie das Crawlen von Websites oder das Sammeln von Inhalten.

Bots können auf verschiedene Weise Schaden verursachen. Kampagnen leiden unter Traffic, der nicht zu Leads, Sales und Kundenbindung führt. Zudem kann Bot-Traffic die Reaktionszeit von Websites verlangsamen, was sich negativ auf die Konversionsraten und das Nutzererlebnis auswirkt.

Bösartige Bot-Aktivitäten können bis zu einem Drittel des Website-Traffics ausmachen[1]. Fortgeschrittene Bots ahmen menschliches Verhalten nach, indem sie z.B. Bewegungen der Maus simulieren. In einigen Fällen können Bots falsche Auslieferungen ausführen, z. B. Ad Injection. Bot-Verkehr kann durch gängige Analyse-Tools und Validierungsdienste identifiziert werden, fortgeschrittene Bots sind jedoch selbst durch ausgefeilte Methoden schwer zu erkennen.

Menschliche Klick-Farmen



Eine Klick-Farm besteht aus billigen Arbeitskräften (meist in einem Entwicklungsland), die von einer kriminellen Organisation dafür bezahlt werden, auf Websites oder Apps zu klicken. Meistens können durch eine riesige Wand aus miteinander verbundenen Mobiltelefonen sehr schnell sehr viele Klicks erzeugt werden.

Wie ihre Bot-Pendants erzeugen menschliche Klick-Farmen Traffic, ohne Leads, Sales und Kundenbindung zu liefern. Zu den angebotenen Dienstleistungen können gehören: Erzeugung von Followern, Likes oder Kommentaren in sozialen Medien, Generieren von Website-Traffic und Klicks auf Display-Anzeigen, Erstellung von Backlinks oder das Teilen von gefälschten Nachrichtenartikeln (Troll-Fabriken).

Fraud durch Klick-Farmen ist schwieriger zu erkennen als einfache Bot-Aktivitäten, da das menschliche Verhalten nuancierter und weniger vorhersehbar ist. Mit Klick-Farmen können Betrüger daher einige grundlegende Maßnahmen zur Verhinderung von Ad Fraud umgehen, die bei der Erkennung von einfachem Bot-Traffic greifen würden.

Quelle: 1) Imperva, Bad Bot Report, 2022;
Cheq, Click Cease blog (2021);
Anura, Click Fraud 101: What every business should know (2022)