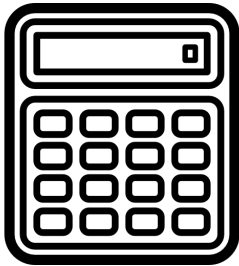




FRAUD TRAFFIC

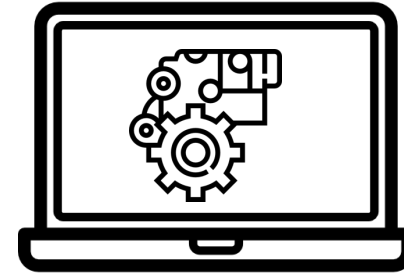


ВИДИ FRAUD TRAFFIC



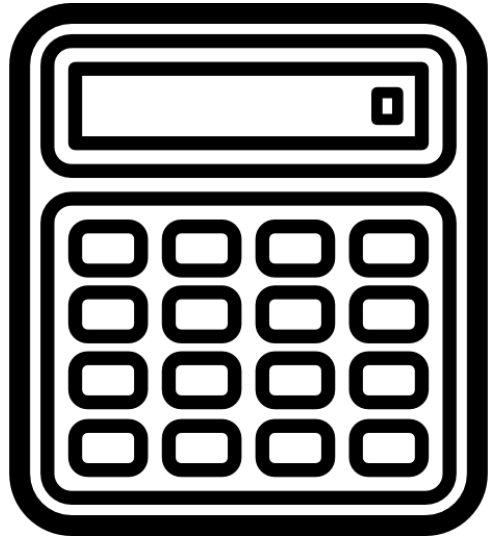
General Invalid Traffic (GIVT)

Базовий недійсний трафік(GIVT) складається з трафіку, визначення недійсності якого проводиться за допомогою рутинних засобів фільтрації, що виконуються за допомогою застосування чорних списків або з іншими стандартизованими перевірками параметрів



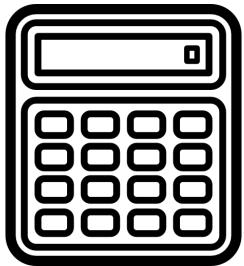
Sophisticated Invalid Traffic (SIVT)

Просунутий недійсний трафік(SIVT) складається з більш важких для виявлення ситуацій, які потребують розширеної аналітики, багаторівневого підтвердження/координації, значного втручання людини тощо, для аналізу та ідентифікації



General Invalid Traffic (GIVT)

GENERAL INVALID TRAFFIC



- **Трафік центрів роботи з даними**

Трафік центрів роботи з даними - це будь-який трафік, який був виявлений за допомогою IP-адресів, походження яких - центри створення та обробки даних

- **Боти/Сканери**

Боти, павуки або інші сканери представляють не людину в Інтернеті. У деяких випадках вони є законними, але все ще не є людьми. Проте навіть законні веб-сканери можуть викликати показ рекламних матеріалів, тому подібні покази також потрібно фільтрувати

- **Підозріла поведінкова активність**

Фільтрація на основі поведінкової активності - це вимірювання активності користувача для позначення дій, які занадто швидко повторюються, з точністю до певного інтервалу, або відсутні дії, які характерні справжньому інтернет-трафіку

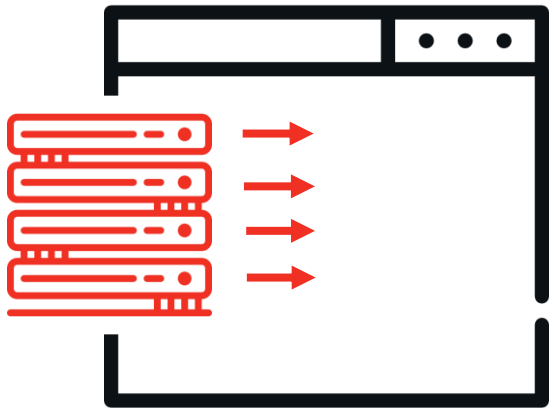
- **Non-browser user-agent**

Вміст поля User-Agent невідомий або нестандартний

- **Попередньо завантажений трафік(pre-rendered)**

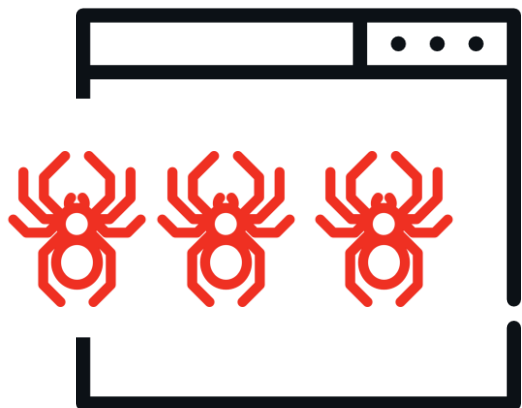
Сучасні браузерери можуть завантажувати вміст веб-сайту до того, як користувач отримає доступ до нього. Проте це попереднє завантаження може призвести до зарахування показу, і такі покази відфільтровуються, коли буде встановлено, що користувачеві фактично не було показано рекламне повідомлення

Трафік центрів роботи з даними



Трафік центрів роботи з даними - це будь-який трафік, який був виявлений за допомогою IP-адресів, походження яких - центри створення та обробки даних

Боти/Сканери



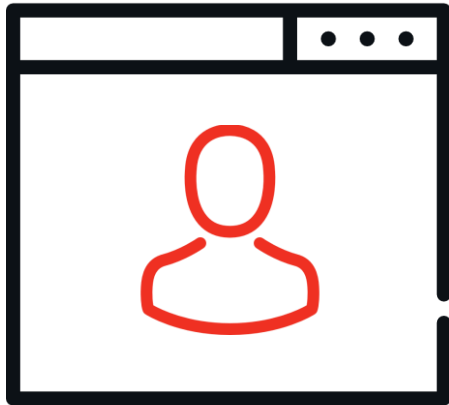
Боти, павуки або інші сканери представляють не людину в Інтернеті. У деяких випадках вони є законними, але все ще не є людьми. Проте навіть законні веб-сканери можуть викликати показ рекламних матеріалів, тому подібні покази також потрібно фільтрувати

Підозріла поведінкова активність



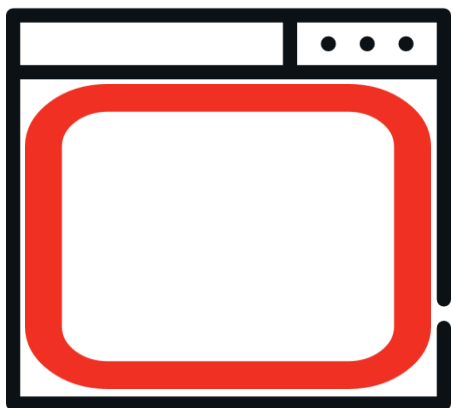
Фільтрація на основі поведінкової активності - це вимірювання активності користувача для позначення дій, які занадто швидко повторюються, з точністю до певного інтервалу, або відсутні дії, які характерні справжньому інтернет-трафіку

Non-browser user-agent

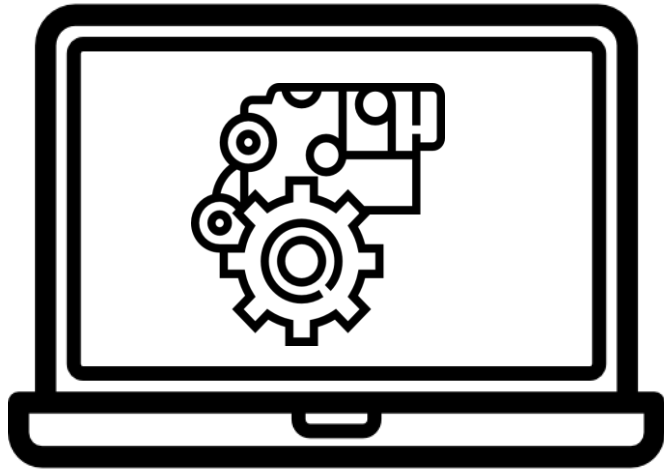


Вміст поля User-Agent
невідомий або
нестандартний

Попередньо завантажений трафік(pre-rendered)



Сучасні браузеры можуть завантажувати вміст веб-сайту до того, як користувач отримає доступ до нього. Проте це попереднє завантаження може призвести до зарахування показу, і такі покази відфільтровуються, коли буде встановлено, що користувачеві фактично не було показано рекламне повідомлення



Sophisticated Invalid Traffic (SIVT)

SOPHISTICATED INVALID TRAFFIC

● Диференціація людського та машинного трафіку

Дійсний та недійсний трафік можуть відобразитись одночасно на одному пристрої. Наприклад, комп'ютер, заражений шкідливим програмним забезпеченням, може автоматично переглядати сайти в фоновому режимі

● Незаконні Боти/Сканери

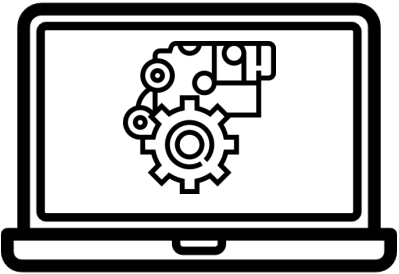
Сервери / машини, створені для накруту трафіку; діють, як велика кількість користувачів для створення подій (переглядів реклами)

● Перехоплення пристроїв, сесій

Шкідливе програмне забезпечення, встановлене на справжньому мобільному пристрої або комп'ютері – це один із способів направити його роботу на підробку законного веб-трафіку на сайт або мобільний додаток

● Недійсний проксі трафік

Використання проксі-сервера дає можливість приховати невалідний трафік



SOPHISTICATED INVALID TRAFFIC

● Adware and malwar

Шкідливе програмне забезпечення, що заражає комп'ютер/девайс з метою фейкових показів реклами під час його роботи

● Маніпуляція з кількісними показниками

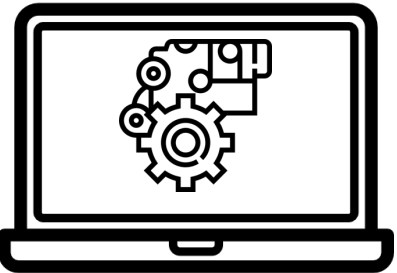
Маніпуляції з кількісними показниками сайту. Наприклад, рекламна платформа може придбати рекламні місця на веб-сайті, а потім залучити трафік на цей сайт, щоб забезпечити перепродажу рекламних місць з прибутком

● Фальсифікація видимих показів

Фальсифікація видимості показів. Показ рекламних повідомлень, які не задовольняють стандартам видимого показу, помилково вважаються видимими

● Підміна домену/формату

Фейковий виклик реклами з підстановкою в лічильник рекламного сервера. Дає рекламному серверу помилкову інформацію про місце показу реклами



SOPHISTICATED INVALID TRAFFIC

● **Зміна cookie**

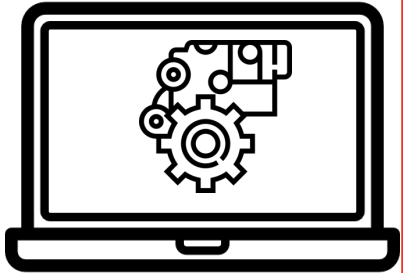
Маніпуляції з файлами cookie користувачів для маскування автоматичних браузерів, шляхом зміни справжніх користувальницьких cookie

● **Маніпуляції з гео локацією**

Фальсифікація даних про місцезнаходження. Справжнє місцезнаходження користувача не відповідає налаштованому гео-таргетингу

● **Невидимий, накладений, захований трафік**

Рекламні оголошення можуть бути приховані за контентом сторінки, можуть бути поза екраном або бути в крихітних 1x1 пікселях, які є невидимими

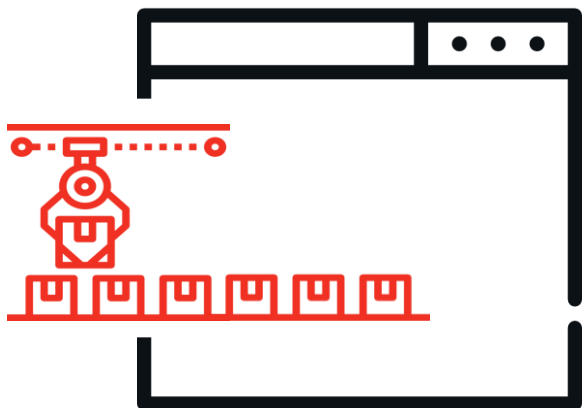


Диференціація людського та машинного трафіку



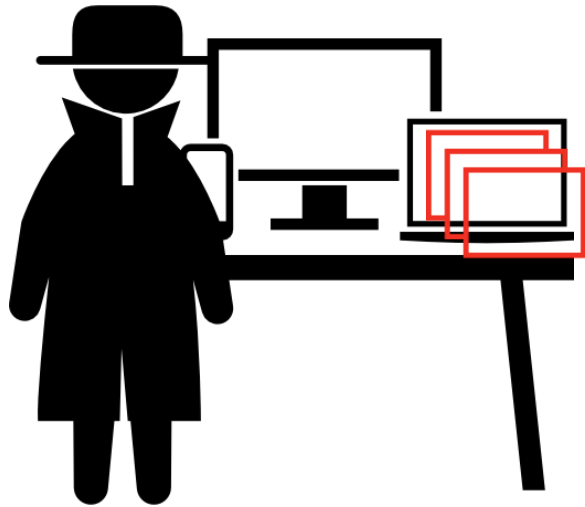
Дійсний та недійсний трафік можуть відобразитись одночасно на одному пристрої. Наприклад, комп'ютер, заражений шкідливим програмним забезпеченням, може автоматично переглядати сайти в фоновому режимі

Незаконні Боти/Сканери



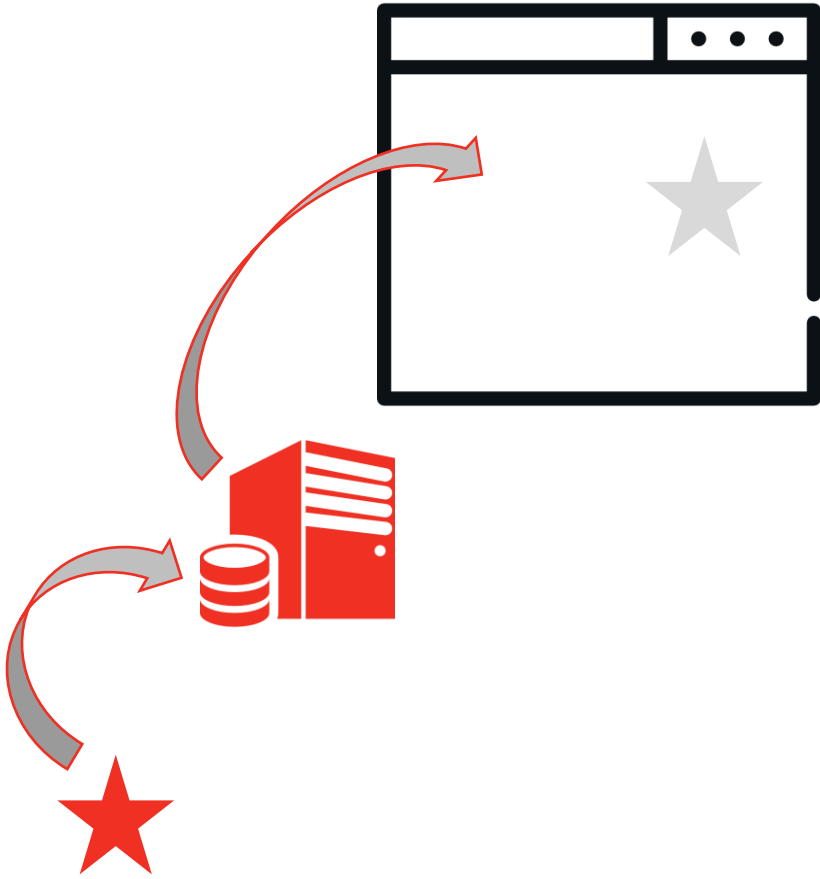
Сервери / машини, створені для накруту трафіку; діють, як велика кількість користувачів для створення подій (переглядів реклами)

Перехоплення пристроїв, сесій



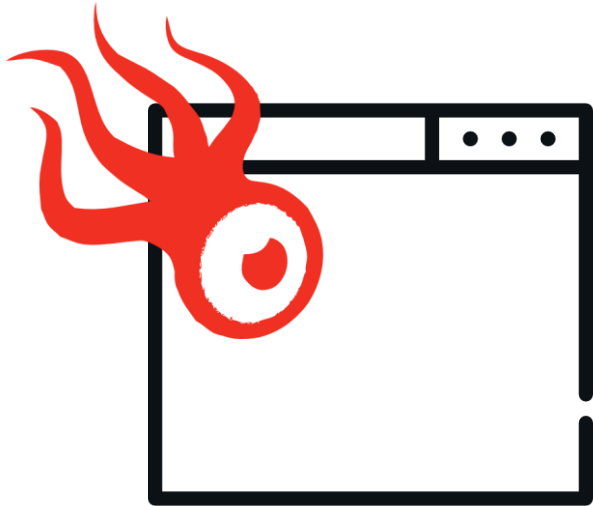
Шкідливе програмне забезпечення, встановлене на справжньому мобільному пристрої або комп'ютері – це один із способів направити його роботу на підробку законного веб-трафіку на сайт або мобільний додаток

Недійсний проксі трафік



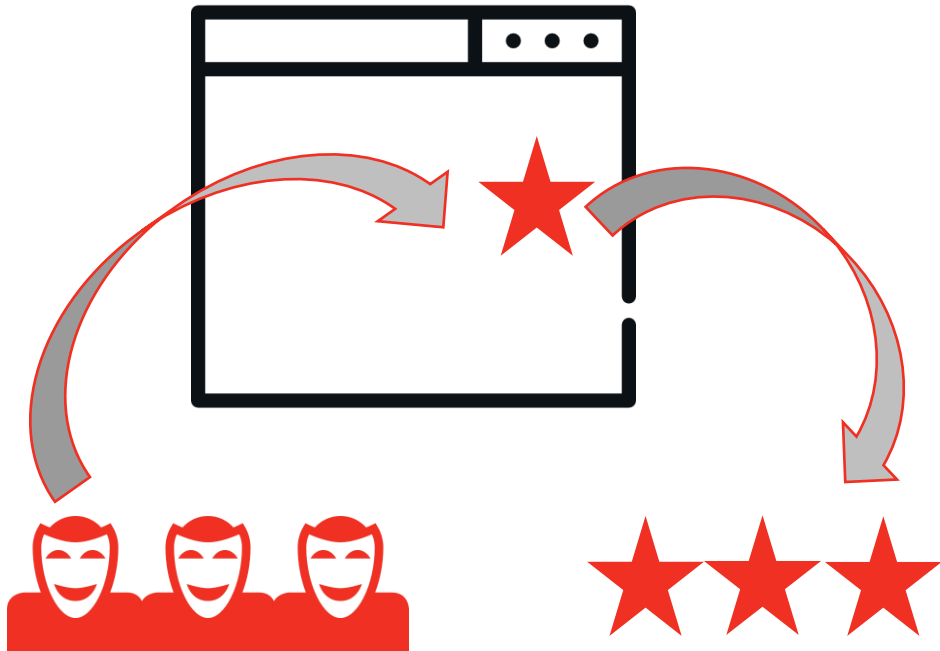
Використання проксі-сервера
дає можливість приховати
невалідний трафік

Adware and malware



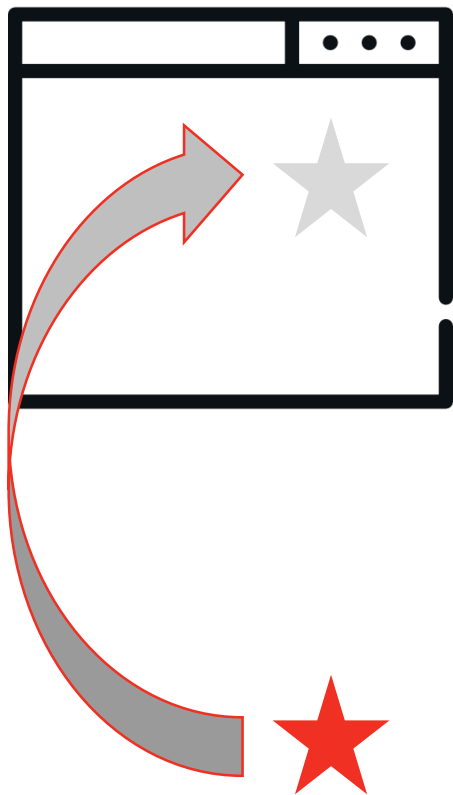
Шкідливе програмне забезпечення, що заражає комп'ютер/девайс з метою фейкових показів реклами під час його роботи

Маніпуляція з кількісними показниками



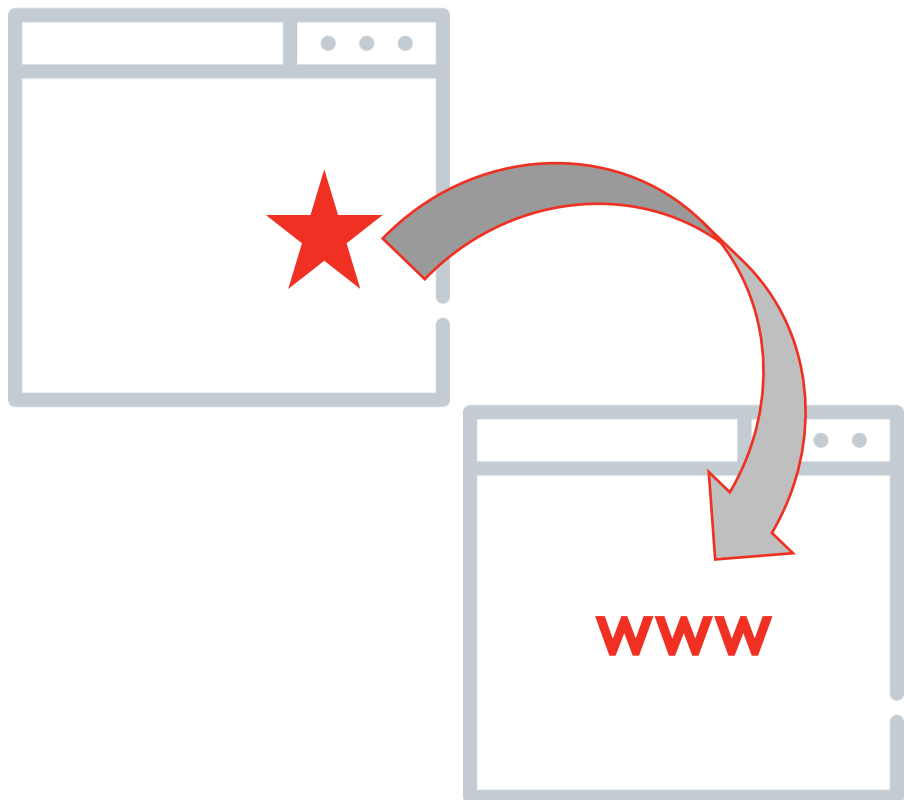
Маніпуляції з кількісними показниками сайту. Наприклад, рекламна платформа може придбати рекламні місця на веб-сайті, а потім залучити трафік на цей сайт, щоб забезпечити перепродажу рекламних місць з прибутком

Фальсифікація видимих показів



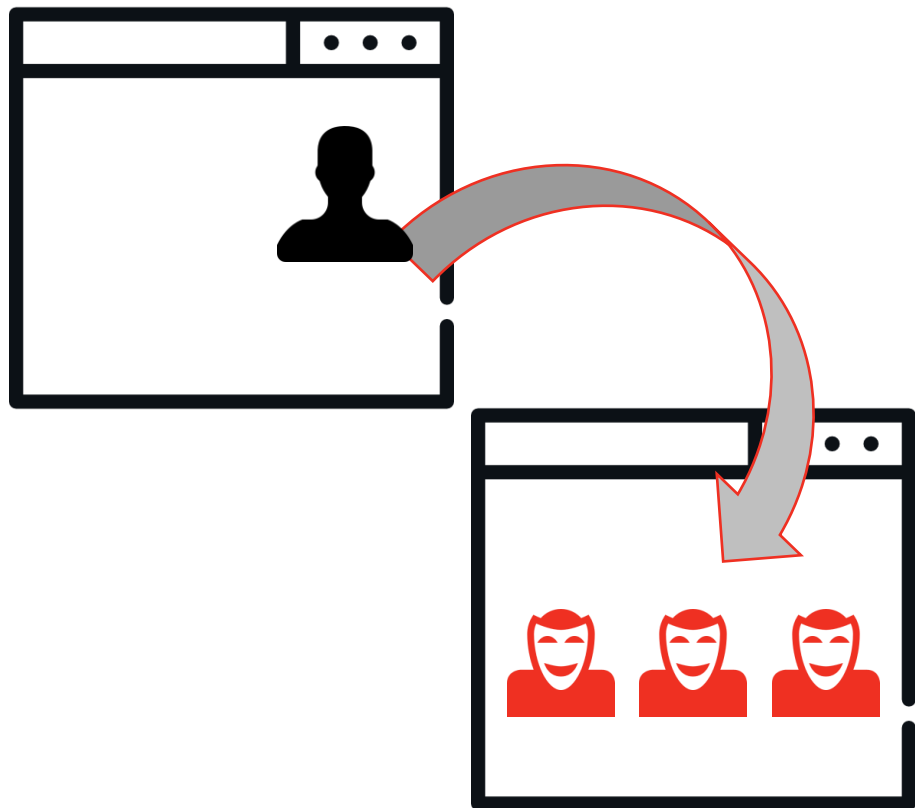
Фальсифікація видимості показів. Показ рекламних повідомлень, які не задовольняють стандартам видимого показу, помилково вважаються видимими

Підміна домену/формату



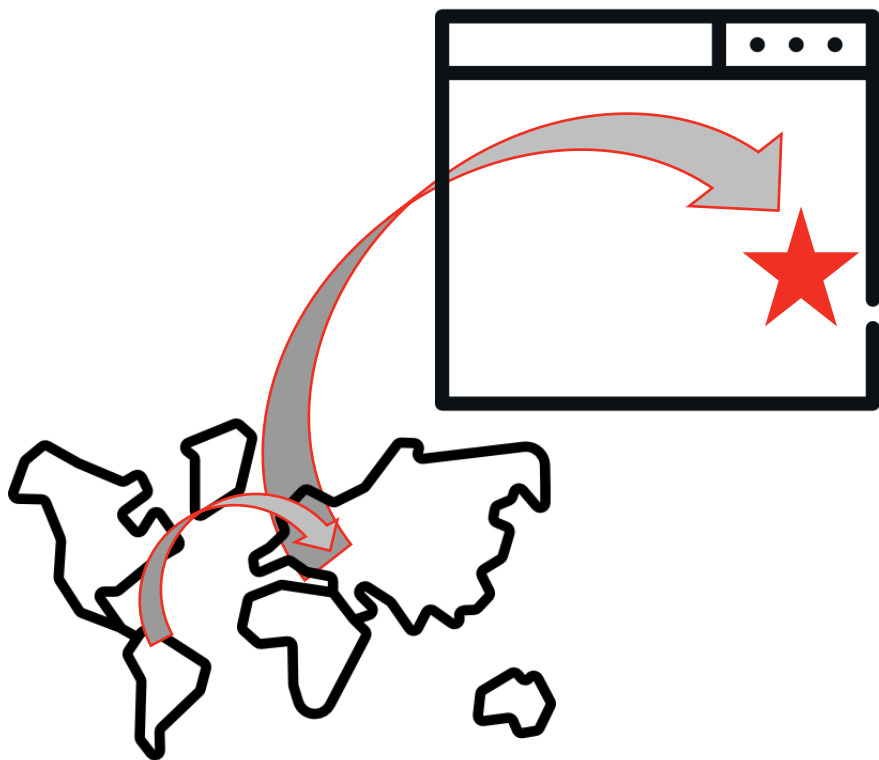
Фейковий виклик реклами з підстановкою в лічильник рекламного сервера. Дає рекламному серверу помилкову інформацію про місце показу реклами

Зміна cookie



Маніпуляції з файлами cookie користувачів для маскування автоматичних браузерів, шляхом зміни справжніх користувальницьких cookie

Маніпуляції з гео локацією



Sophisticated Invalid Traffic

Фальсифікація даних про місцезнаходження. Справжнє місцезнаходження користувача не відповідає налаштованому гео-таргетингу

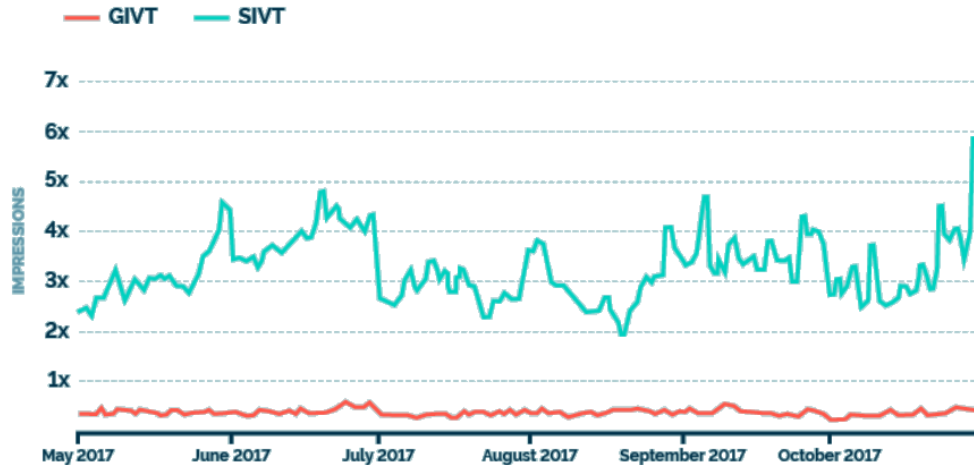
Невидимий, накладений, захований трафік



Рекламні оголошення можуть бути приховані за контентом сторінки, можуть бути поза екраном або бути в крихітних 1x1 пікселях, які є невидимими

Співвідношення GIVT та SIVT

GIVT vs. SIVT traffic levels



GIVT - це як білий шум, який завжди на фоні. І кількість контактів з ним набагато нижча, ніж у SIVT.

З іншого боку, SIVT - це постійно еволюціонуюча система, де шахраї намагаються розробити нові форми шахрайства, які поєднуються з законним інвентарем без виявлення. SIVT представляє більшу загрозу бюджетам рекламодавців, ніж GIVT, як з точки зору обсягу, так і його здатності маскувати себе як законний трафік.