ENSIGHTEN

Ensighten eGuide

The Impact of Ad Injection on Online Customer Experience

An increasing number of organizations are seeing a dramatic drop in revenue and online conversion rates, due to customers being lured away to competitor websites via fraudulent ad injection

August 2019

Introduction

The role of your website in determining the success and growth of your business cannot be underestimated. It acts as a shopfront, a trading platform, a goldmine of valuable customer data, and, it projects an image of your organization to the rest of the world.

As one of the channels upon which you rely to generate business, you have no doubt invested significant resources in optimizing the look, feel, and user experience in order to provide a seamless, engaging experience for web visitors. However, many websites are facing a growing threat; unauthorized ad injection.

Ad injection is the process where unauthorized ads are injected into your website visitors' browsers, diverting them to your competitors' websites, losing you valuable sales and providing a frustrating online experience for your customers – all without your knowledge. In fact, these cyberattacks typically go undiscovered.

Ad injection explained

Better known as a form of 'malvertising'; a third party can inject unwanted software, malware or adware into your website visitors' browsers without permission. It allows customers to be targeted by unauthorized ads which plague their online journey with product ads, pop-ups, banners and in-text redirects, at best disrupting their experience and driving them to competitor websites.

The process is based on adware – either disguised as legitimate software or piggybacking on another program to mislead your website visitors into installing a program onto their PC, tablet or mobile device.

Ad injection is based on adware, either disguised as a legitimate software or piggybacking on another program to mislead your website visitors

Once adware hijacks the user's device, it might be used to analyze their online behaviour, including their browsing history, to re-direct them elsewhere. Worse, the adware creators often sell this information to other third parties, resulting in further customized and competitive ads.

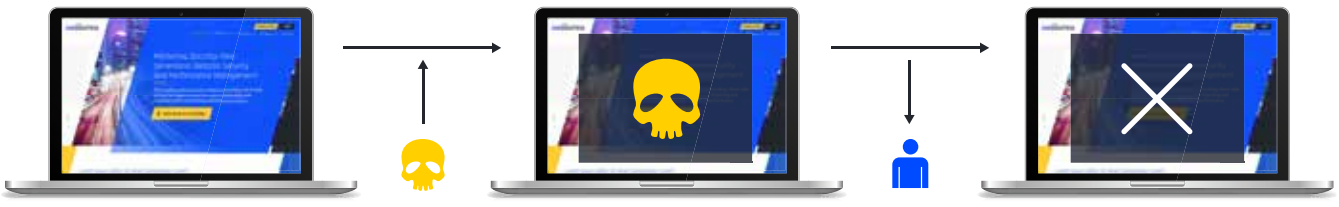
48% ***of malware today is used to auto-redirect users to another website***

Ad injection is an increasing problem. Every 60 seconds, close to $1.14m is lost to cybercrime, according to a report by threat management firm RiskIQ. Alongside threats from malware, phishing and supply chain attacks that target third parties, the report notes that cybercriminals deploy more than nine malicious adverts every minute.

Specifically, malware that auto-redirects a user to another site is by far the most used scheme to disseminate malvertising today, representing 48 percent of malware. One 2018 estimate put the cost to the online advertising industry at more than $1.1 billion a year, rising another 20–30 percent in 2019.

A third party can inject unwanted software to target your website visitor with unauthorized ads that disrupt their experience and drive them to competitor websites

Without the Ensighten solution



User visits your website and adds items to shopping cart

Meanwhile, competitor advert is injected into your site

User is presented with a competitor advertisement, using compelling offers to attract your visitor to click on the advert

Potential customer leaves your site to transact with your competitor

This leads to lost revenue and poor user experience

Why is ad injection so damaging for your business?

Any interruption that diverts customers away from your website will result in fewer online conversions and transactions, thus damaging your ability to retain customers.

74% ***of shoppers will only wait 2-3 seconds for a page load before leaving to shop on another site***

It has been suggested that consumers' attention spans are decreasing – 74 percent of shoppers are only willing to wait two to three seconds for a page to load before leaving to shop on another site. Interruptions such as ads, pop-ups and videos are likely to have your website visitors immediately reaching for the back button.

This type of attack can be harmful to your business on many levels:

Lost revenue

The fraudulent ads redirect your customers to other retailers, resulting in abandoned shopping carts and lost revenues

Online experience

Unauthorized ads create a frustrating online experience for your customers, damaging your brand's reputation

Website performance

If adware-based cryptocurrency mining software is injected, it can significantly affect website performance

Ad injection for theft

In some cases, your customers' personal information can be compromised, or the infection can deliver malware to the user's computer.

In 2018 security vendor Check Point uncovered an extensive malvertising campaign that had ties to legitimate online advertising companies. A hacker group used more than 10,000 compromised WordPress sites and multiple exploit kits to spread a variety of malware, including ransomware and banking Trojans. The group, which Check Point labelled Master134, used unpatched WordPress sites that were vulnerable to remote code execution attacks and then redirected traffic from those sites to pages run by ad networks. These in turn redirected users to a malicious domain that downloads malware to users' systems.

In addition, incidents of ad injection often spike during the holidays when online shopping is at its peak and IT or web teams may not be available to troubleshoot any problems. One large malvertising campaign hit US users over the extended Presidents' Day weekend in 2019, according to Confiant, which tracks bad ads. Researchers say they've seen as many as 800 million malicious ad impressions as part of the campaign, which redirected users to a range of malicious sites. In this instance the goal of the hijacking was to trick users into entering their personal and financial information into checkout forms for non-existent products. Similar to formjacking, the cybercriminals collect these details and to sell on the dark web or use them for other fraudulent purposes.

Any interruptions that distract customers away from your website will result in fewer online conversions and transactions

Could you be next?

Any size of organization can fall victim to this type of attack and these unauthorized ads are not exclusive to any one industry, geography or phase of the online journey. In addition, incidents such as these look set to continue with the proliferation of mobile devices, with adware making its way into mobile apps.

Amazon was targeted by a "sophisticated and widespread" scheme in 2018, designed to deceive consumers into interacting with malicious ads and websites. The ads and popup messages, which appeared to visitors to be affiliated with the Ecommerce giant, were created to generate fraudulent advertising revenue and obtain the personal information of online consumers by taking advantage of the company's brand recognition.

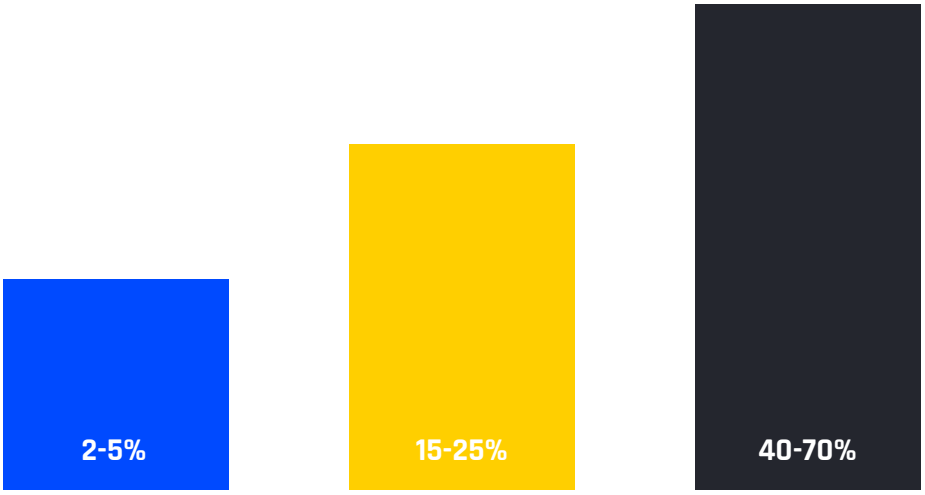
Hiding in plain sight

The whole process happens away from your web servers and at the client-side, so as a website owner, you are likely to have no visibility into the damage that is being inflicted on your organization. Because the malware resides on the user's browser or device, traditional server-side security solutions lack visibility or control over the problem. Therefore, you may be having your revenues stolen without ever being aware there is a problem.

Because the malware resides on the client-side, traditional server-side security solutions lack visibility and control over the problem

As a website-owner you have no visibility into the damage that is being inflicted on your organizations since the whole process happens away from your web servers

The cost of unauthorized ad injection



Ad injection is estimated to cost businesses between 2-5% in annual revenue

15-25% of all user web sessions are exposed to unauthorized ads

In 40-70% of incidents, the ads feature competing promotions that divert users to competitor website

What's the solution?

Our ad injection prevention solution enables you to detect, manage and block any unauthorized advertising and malware injected into visitor sessions and stop your customers from being diverted to other websites. We will enable you to:

- Keep your website visitors on your site to increase conversion rates
- Prevent stolen revenue through blocking potential diverted web visits
- Decrease your shopping cart abandonment figures
- Enhance and protect customer experience through a distraction-free online journey
- View attempted ad injections on your website in real time
- Block ad injection, adware and malware on your website

As part of our ad injection prevention solution, you will gain access to the full Ensighten MarSec™ platform, giving you the ability to extend your client-side website security to prevent data leakage and cyberattacks through your third-party website technologies - without impacting the online customer experience.

Don't take the risk of losing your hard-earned revenue to the competition or cybercrime. Speak to Ensighten about how we can help ensure your customers' data remains protected, their online experience with your website is seamless and distraction-free, and your business continues to thrive.

> ***"Ensighten has not only ensured that our website is protected from client-side data leakage and cyberthreat groups, but also enabled us to block malicious and competitive advertising which had effected our conversion rates and revenue. We saw an immediate uplift in conversions and sales as soon as we implemented the solution."***
>
> — Leading global retailer

With the Ensighten solution

User visits your website and adds items to shopping cart

Meanwhile, Ensighten blocks all unauthorized adverts from appearing on your website

The user continues with online shopping experience to transact

There is no disruption from competitor ads or adware

You retain control of revenue and customer experience on your website

About Ensighten

Ensighten is a global cybersecurity leader, offering next generation client-side protection against data loss, ad injection and intrusion. Through the Ensighten solution, organizations can assess privacy risk and stop unauthorized leakage or theft of data, as well as comply with CCPA, GDPR and other data privacy regulations. Ensighten's MarSec™ platform protects some of the largest brands in the world from data leakage whilst ensuring maximum web page performance.

Ensighten is headquartered in Menlo Park, US with the European HQ in London, UK. To learn more visit www.ensighten.com and join the conversation on LinkedIn and Twitter.