The Impact of Customer Journey Hijacking on E-Commerce Q4 Sales in the U.S.

SEPTEMBER 2017

NAMOGOO

PREVENTING JOURNEY HIJACKING

Introduction

The holiday season between November 1 and December 31 is the busiest time of the year for retailers. In 2016, during this period alone, online sales hit $91.7 billion, up 11% from $82.5 billion the previous year.

The 2016 holiday season broke a major e-commerce record: Cyber Monday became the biggest online shopping day in U.S. history, generating $3.45 billion in online sales, up 12% from the year before. And the 2017 holiday season is expected to hit even higher numbers.

It is not surprising that retailers work extra hard during Q3 to optimize the shopping experience and to capitalize on the increased traffic expected in this critical time of the year.

However, a new threat is putting retailers at an estimated loss of $2.1 billion during the anticipated 2017 holiday season.

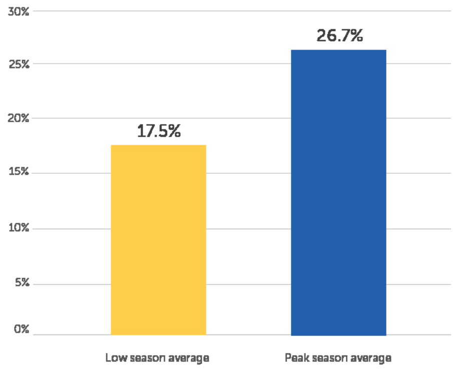
This report provides an overview of customer journey hijacking based on an analysis of 500 million page views per day from top e-commerce sites across all product categories. Namogoo monitored these sites on a daily basis over a period of 12 months.

Customer Journey Hijacking, a Real Threat to Online Retailers

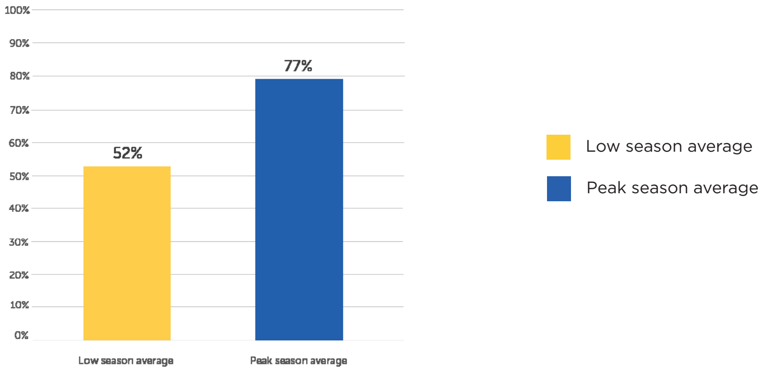
Customer journey hijacking exists across the web, yet the majority of retailers are unaware of this major threat to revenue. Unauthorized product ads that are injected into consumer browsers compete with retailers, distracting prospects from their offerings and cutting directly into their revenue. On top of all this, the customer experience is harmed by the distracting and sometimes unsavory content littered across the site.

The sheer number of online consumers affected on a daily basis by journey hijacking is staggering. During the non-holiday shopping season, **15-25% of user sessions are interrupted by unauthorized ads, and in 40-70% of these cases, the ads feature competitive products that hijack** the customer to the retailer's competitors. These figures increase dramatically during peak shopping seasons, as indicated in the charts below:

% of customer sessions with unauthorized ads



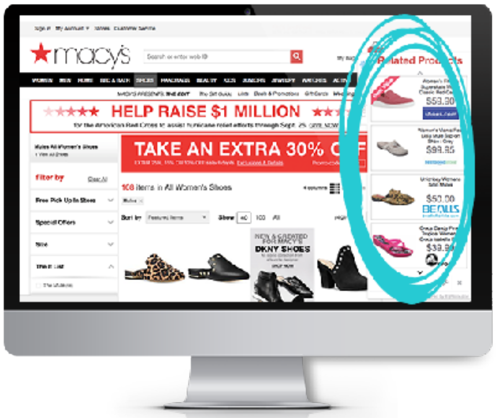
% of ads featuring competitive products



The following examples include screenshots of infected browsers and illustrate how customers will experience retailer sites:

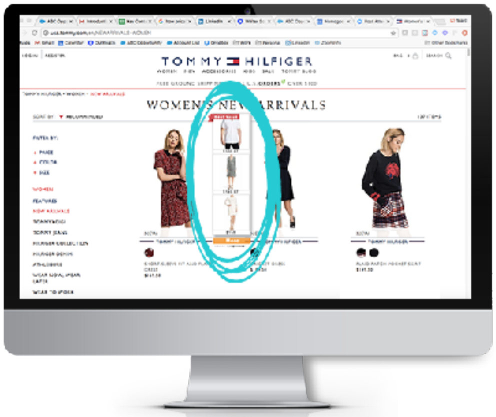
Example 1

Related products ad on a category page. This script identifies where the customer is browsing and shows users relevant competitive product advertising.



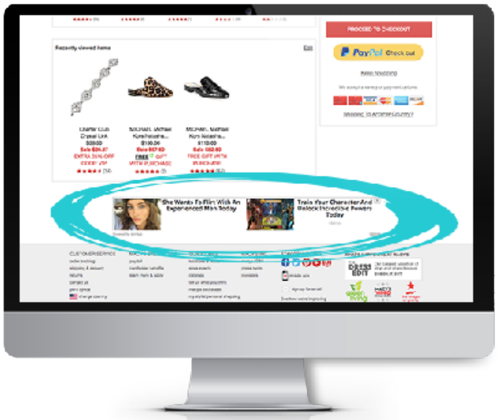
Example 2

Related products ad injection. This script pushes the ad to the center of the page, gaining high visibility and higher click rates.



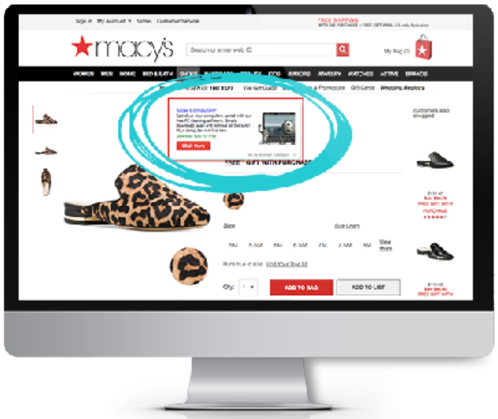
Example 3

Banner ad at the checkout page. This ad diverts the customer from completing the order at the most important stage of the buying process.


Proceed To Checkout
PayPal Check out
She Wants To Flirt With An Experienced Man Today
Train Your Character And Unlock Incredible Powers Today

Example 4

In-text ad on product page. This ad looks for keywords on the page and transforms them into external links. It can also hijack existing links and redirect the customer to competitor sites.



These injected ads are caused by digital malware that is often bundled in software your customer downloads (e.g., a free PDF viewer or even – as ironic as it may seem – an anti-virus program), or added via updates to other programs already installed on their computer, such as browser extensions. They can also unknowingly become infected via public Wi-Fi connections. All of this happens without your customer even noticing. Infections can occur across all browsers, operating systems, and devices (including mobile phones and tablets), and such sophisticated digital malware manages to impact even your most tech-savvy customers.

Once malware has infected a browser, it injects unauthorized widgets (product recommendations and deals), advertisements, and spyware scripts.

The websites that the customer views now appear far different from what was intended, littered with third-party ads that the retailer did not agree to or receive payment for. That third-party becomes a leech, making money via clicks on the unauthorized ads, selling competitive products, and getting paid affiliate commissions for directing users right back to the original website. This type of malware runs in a layer on top of the webpage, bypassing servers and website security, and is therefore completely outside the control of the website owner.

Where Ad Injections Take Place

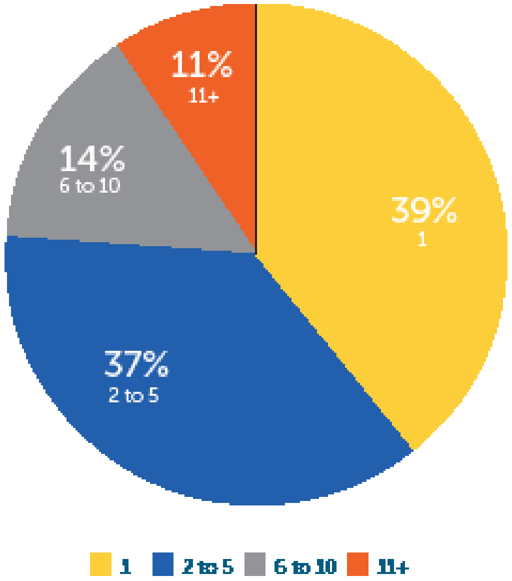
Unauthorized ads can appear on all web pages. However, most injections (about 70%) occur on product, shopping cart, checkout, and account pages, but not on the homepage, even though it is usually the most visited page of a website. Of that 70%, about 10% occur on checkout or shopping cart pages, leading to increased cart abandonment rates.

The Holiday Rush: A Busy Season for Everyone...Even Hijackers

To make matters worse, these digital interruptions and distracting pop-ups increase exponentially during the holiday seasons. Just as online retailers invest substantially in making this time of year as profitable and enjoyable for their customers as possible, malware developers are pulling out all the stops to increase their reach and optimize their ads to generate more clicks and revenue. So while you are devoting time, money, and energy to increasing your sales revenue, conversion, and customer retention, malware is working its hardest to take those things away from you.

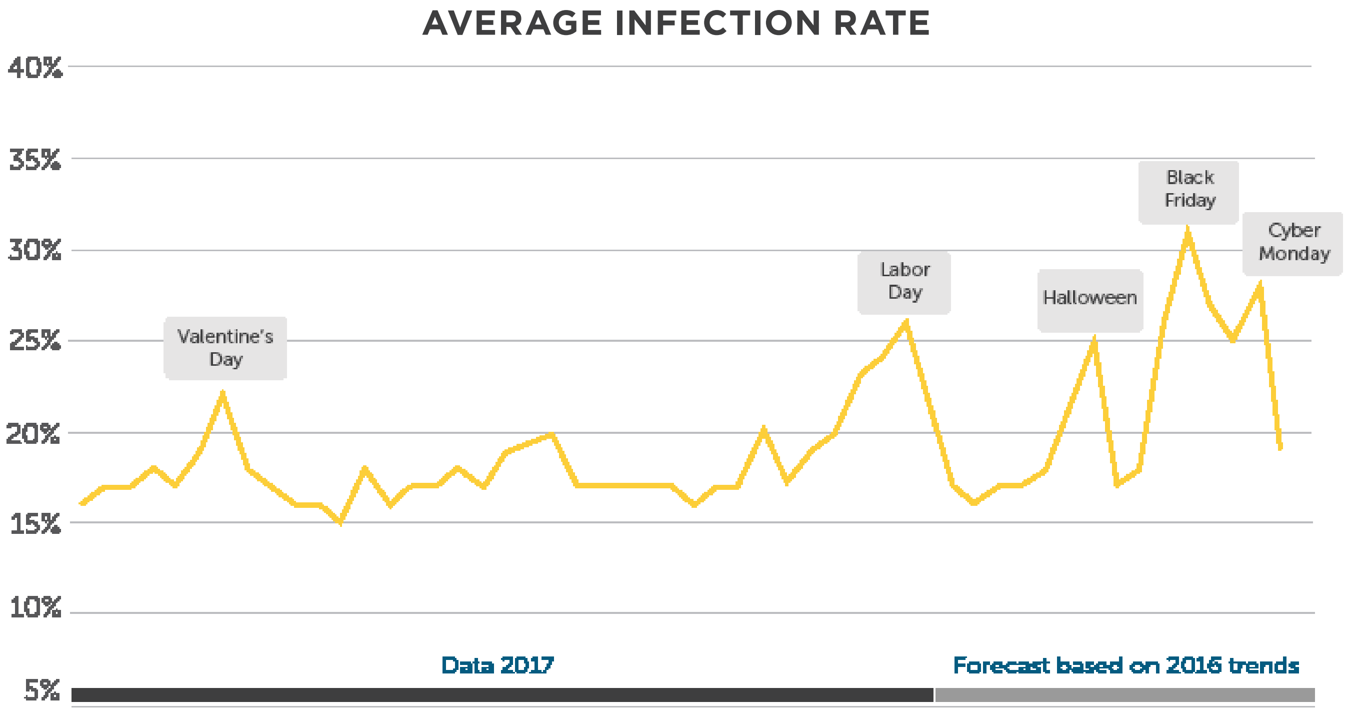
FIRST INFECTED PAGE VIEW

A session is most likely to get injected with unauthorized ads on the first page view (39%) or between the second and fifth pageviews (37%).



Around the holiday season, figures show that customer journey hijacking increases to affect 20-30% of all sessions. Additionally, of those sessions, 80% of the displayed ads are for competitor sites, effectively driving qualified seasonal traffic from your online retail site directly onto the site of your competitor. The amount of lost revenue resulting from such tactics is astronomical and can be devastating, particularly at such a pivotal shopping time as the holiday rush.

According to analysis based on last year's rates, infection prevalence is projected to remain steady at the 15-25% mark in September/early October, and increase exponentially during the busy shopping periods such as Black Friday, Cyber Monday, and Christmas.



Namogoo: Journey Hijack Prevention to Win Back Stolen Revenues

Namogoo is pioneering the market of journey hijack prevention. Namogoo's disruptive technology is designed to identify and block unauthorized product ads that are injected into web sessions, diverting the customer journey and damaging conversion rates. By eliminating these invasive promotions, Namogoo consistently recovers revenue for online stores;. Fortune 500 companies that use Namogoo report an immediate conversion uplift, and are able to win back more than 90% of their stolen revenue.

To see the impact of online hijacking on your own customers, contact us for a free website analysis.

BOSTON
745 Atlantic Ave
Boston, MA 02111
USA

ISRAEL
7 HaSadna St.
Ra'anana 4365004
Israel

NAMOGOO

namogoo.com 857.284.8084