NAMOGOO

ECOMMERCE MARKETING HANDBOOK

Protect Your Digital Investments:

How to Stop Customer Journey Hijacking from Stealing Your Online Revenue

Introduction

Today's major retailers know that thriving in the world of eCommerce involves more than an impressive online product catalog and a secure, functional checkout webpage. It requires companies to offer comprehensive online experiences that bring consumers in and prepare them to open their wallets.

That's why so many retailers are willing to invest in building a robust eCommerce operation, including an attractive website and a variety of other online marketing assets.

But a significant portion of these investments typically go to waste.

That's because, in many cases, when a consumer reaches a retailer's eCommerce website, that individual will not experience that site the way the retailer had planned. Worse yet, the retailer may not even realize the discrepancy.

Today, bad actors use client-side threats such as malware and Wi-Fi hijacking to display injected ads to online shoppers during 15% to 25% of user sessions. These ads are intended to steal consumers away and redirect them to competing websites—and they are remarkably effective, jeopardizing sales revenue and undermining your marketing investment in both the short term and the long term. That's what we call Customer Journey Hijacking (CJH).

This eBook will help you protect your online marketing investments from these threats, preventing CJH from achieving its goals. In the following pages, you will learn:

- How client-side threats steal away your customers through Customer Journey Hijacking.
- Who the bad actors behind CJH are and how they make money.
- How CJH targets the most promising consumers at the most promising times.
- How CJH impairs a retailer's ability to achieve strong online KPIs.
- How you can kick injected ads out of your online store **before** CJH sends your customers straight into the arms of your competitors.

Table of Contents

CHAPTER 1:

How Do Client-Side Threats Steal Away Your Customers?

Imagine the following scenario: It's Black Friday, and your brick-and-mortar store is bustling. Your 10 cashiers are doing their best to keep up with the pace of customers, but the line at each register keeps growing.

You watch as a customer approaches a cashier with a cart full of merchandise that she wants to buy. But instead of ringing up the sale, the cashier takes a good look at the items in her cart and tells her she can get better deals at the competing store across the street from yours.

Suddenly, you realize the man sitting at the cash register isn't a cashier at all. He's an imposter—and so is the "cashier" at the register next to his. While you weren't watching, these two strangers walked into your store, impersonated your employees, and started redirecting your shoppers to competing stores.

Sound outrageous? It's essentially what Customer Journey Hijacking does to retailers every day—except that usually the retailers don't notice the imposters. In fact, during Q3 of 2019, the data we gathered from our customers showed unauthorized ads appearing during 16.40% of eCommerce sessions in the U.S. and 17.97% of eCommerce sessions in Europe.

How does Customer Journey Hijacking work?

While there is some variability in the ways Customer Journey Hijacking occurs, it is usually executed through a three-step process:

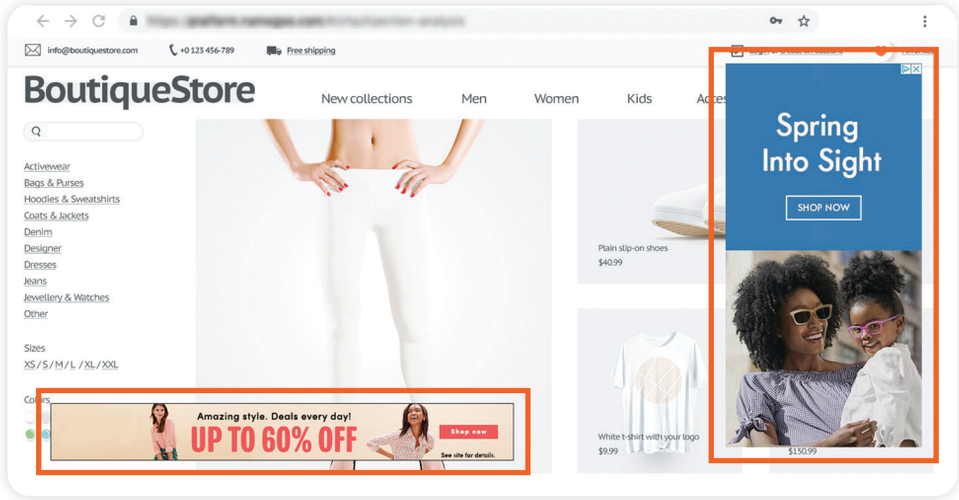
1. Malware is secretly installed on the user's digital device. (In most cases, this happens when they download free software such as a mobile app or browser extension.)
2. The malware tracks the user's online activity, building a personal profile reflecting their shopping preferences and habits.
3. When the user visits an eCommerce website, the malware automatically displays injected ads. (Alternatively, this ad injection can occur via Wi-Fi hijacking, exposing even users who have not downloaded malware to the risk of CJH.)

Who is targeted by Customer Journey Hijacking, and when?

As CJH continues to impact online retailers, there is a growing awareness of injected ads and how they steal customers away, resulting in lost eCommerce revenue. But many people assume that the online visitors most affected by CJH are those who are less tech-savvy and less likely to spend significant money online.

In fact, the numbers show that just the opposite is true: The consumers who have the highest eCommerce KPIs are far more likely to have their digital devices infected with the malware that drives injected ads.

Examples of Ads Injections



Namogoo's analysis of hundreds of millions of web sessions per week shows that consumers who spend more time (and money) shopping online are more likely to download free software (such as browser extensions and mobile apps) that may be bundled with malware. As a result, these users are more likely to have ads injected into their browsers.

What that means for retailers is that CJH can be more damaging than general statistics suggest. Injected ads don't simply appear during 15% to 25% of visits to a retailer's online store—these ads affect a significant portion of that retailer's most promising customers and prospective customers.

In addition, it is important to keep in mind that Customer Journey Hijacking affects shoppers on both desktop (or laptop) computers and mobile devices such as smartphones. According to the data we gathered from the eCommerce companies we work in Q3 of 2019,

injected ads appeared during 13.99% of mobile shopping sessions in the U.S. and 17.18% of mobile shopping sessions in Europe. Although these numbers are lower than the corresponding figures for desktop shopping sessions, mobile users are typically less patient when it comes to disruptions.

Who carries out Customer Journey Hijacking, and why?

At its core, the profitability of CJH depends on the profitability of affiliate marketing. That's because of the business model of affiliate networks—a model that is supposed to rely on mutually beneficial relationships in which customers get good deals on products they want, businesses sell their goods and services to those customers, and affiliates get paid for directing interested consumers toward the products they want. By effectively connecting retailers, publishers, and shoppers, affiliate networks have been able to create a powerful platform for customer acquisition, specifically catered to the special demands of online retailers.

But Customer Journey Hijacking takes advantage of that model, discreetly redirecting traffic from one website to another and then charging the owner of the receiving website an affiliate fee. Meanwhile, the companies whose websites receive traffic acquired through CJH are typically unaware of the unscrupulous methods that have brought them prospective customers.

As a result, your competitors may well be unwittingly selling products to customers stolen away from your website by injected ads.

In addition, if you have an online store, there could be another, less obvious way CJH hurts your bottom line: Ad injectors may display affiliate ads for discounts on your own products. Then, when a shopper clicks on one of these ads, they will be automatically redirected back to your website. In "return" for the visitor that the ad injector has "brought" to your store, the company behind this malware may then charge you an affiliate fee.

In other words, there's a good chance that ad injectors are charging you money for traffic that is already on your website.

CHAPTER 2:

How Does CJH Impact the Key Objectives of Online Marketing?

As we have seen, the main reason that Customer Journey Hijacking continues to plague retailers is that these companies are so willing to pay for their online traffic—in this case, through the affiliate fees that make CJH profitable. That same willingness is reflected in the other key investments in online marketing for which major retailers are happy to shell out, such as website optimization, paid advertising, and the work hours required to build a robust social media presence.

Unfortunately for online retailers, affiliate fees are just the beginning of the cost of ad injections.

In addition, these client-side threats reduce the ability of eCommerce websites to achieve their main objectives—effectively diminishing the value of all of a retailer's online marketing assets.

While some of the harm is easy to measure in terms of KPIs, other significant aspects of this damage are more difficult to quantify.

Here are three realms in which client-side injected ads can be particularly costly for retailers:

1. **Sales revenue**

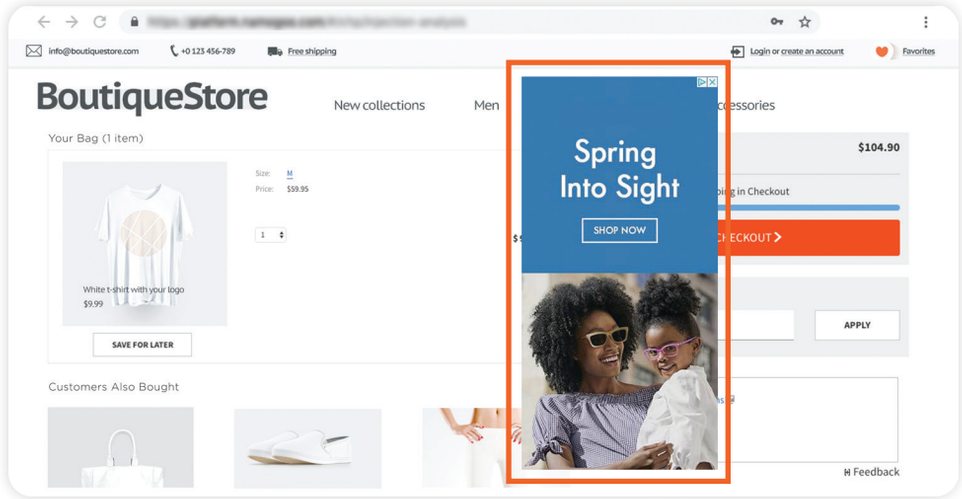
   The most common way that Customer Journey Hijacking hurts retailers is by guiding prospective customers straight into the arms of their competitors—often depriving a victimized retailer of a sale for which that company has already invested significant resources.

At Namogoo, we have found that promotions for products offered by competing stores account for 60% to 65% of the injected ads that target customers of the retailers we work with.

And as bothersome as these injected ads can be throughout the customer journey, **they are particularly problematic when they appear at the very bottom of the sales funnel—which is exactly where they are most likely to show up.** In fact, our large-scale data analysis found that these ads appear during 28.99% of visits to checkout pages and a whopping 40.43% of visits to order confirmation pages. It seems that the ad-injecting malware that drives CJH makes a point of targeting shoppers who are already ready to pay.

What do these numbers tell us about the malware that drives injected ads? For starters, we can see that ad injectors tend to target the most promising shopping sessions. By injecting ads specifically into pages that typically are only accessed by those consumers who

Example of an Injected Ad on a Checkout Page



are serious about making a purchase, these ads aim to nab the most interested shoppers. This approach also means that if a consumer is stolen away from one online store to a competitor, the competitor may well benefit from everything the first store has done to prepare that individual to make a purchase.

Adding to CJH's tendency to hurt sales numbers, injected ads often increase page loading times by requiring digital devices to process and transmit more information. In some cases, CJH can even cause a website to freeze or crash—a customer experience catastrophe, especially among consumers who may be choosing eCommerce specifically because of its speed and efficiency. And 3% of ad injections feature videos, increasing the chances of slow loading, freezing, and crashing.

Having to wait a number of seconds for a website to load may sound less shocking than viewing ads for competing products, but slowly loading web pages pose a costly problem for retailers. Considering the mindset of online shoppers, it's not hard to see how slow page loading could damage the customer experience.

As a result, even if your customers aren't clicking to be redirected to your competitors, a frustratingly slow customer experience could slam the door shut on a sale.

2. Brand reputation

If you think ads leading to your competitors are harmful, think of the damage that could be done to your brand reputation by the other 35% to 40% of ad injections.

Of the injected ads that we at Namogoo have identified and blocked, we have found that:

10%
promote adult websites.

5% to 10%
are designed to mimic legitimate alerts (such as error messages or recommendations from the user's operating system) in order to trick users into clicking on them.

15% to 20%
promote online gambling or gaming.

Worse yet, consumers who view ad injections while visiting a website typically think these ads are coming directly from the site, rather than running on their own digital devices. As a result, if a shopper is in your online store when an injected ad appears, they are likely to blame your company.

In fact, in our survey of more than 1,300 online shoppers, 78% of respondents said that if they were exposed to an injected ad while shopping on an eCommerce site, they would view that retailer negatively because of this interaction.

This study also found that 66% of consumers think that if they are visiting an eCommerce website when pop-ups, banner ads, and product ads appear, that indicates that their privacy is being compromised. And perhaps most shockingly, only 3% of consumers said that if they are visiting an eCommerce site when a pop-up for a competitor appears, that is a result of a bug on their own device rather than a problem caused by the website.

3. Customer retention

Each time a customer is tempted by an injected ad, there's a real chance that shopper could disappear forever. In fact, in our study of online shoppers, 58% of respondents said that if they were shopping in an online store when they saw a pop-up ad for a competitor selling the same product at a lower price, they would

likely click the ad. And 80% said that if they ended up buying from the competing store instead of the first store in this scenario, the competing store is the one they would be more likely to visit the next time they are looking for a similar product.

Part of the problem with CJH is that it sabotages eCommerce sales through a combination of “push” factors and “pull” factors. While ads for similar products at lower prices could pull a shopper into a competing store, offensive ads and slow page loading times can push consumers away.

Not only does this combination of factors hurt online sales, but it can wreak havoc on customer relationships. Considering the cost of acquiring a new customer and the fact that repeat customers tend to spend more, the damage caused by injected ads can be both significant and irreversible.

CHAPTER 3:

How Can eCommerce Companies Take on the Ad Injectors?

One of the main reasons Customer Journey Hijacking has become so prevalent in recent years is that conventional cybersecurity measures are incapable of stopping it. Because client-side threats such as injected ads are not part of your website, you cannot see them directly. And because you cannot control your customers' Wi-Fi connections or prevent malware from being installed on their digital devices, you cannot eliminate the causes of CJH entirely.

So what can you do to protect your online store from injected ads? Today, it is possible to automatically identify and block ads from appearing on users' digital devices through the innovative use of artificial intelligence.

As a result, today's retailers have a viable and effective option for fighting ad injections: Customer Hijacking Prevention (CHP).

At Namogoo, we specialize in empowering retailers to keep injected ads away from their shoppers through Customer Hijacking Prevention. We ensure the effectiveness of our CHP solution by continuously conducting A/B tests measuring our technology's impact on our customers' KPIs. While much of our testing focuses on specific companies, this work has also provided us with some important general insights. Our findings include:

- Retailers that use our CHP solution typically achieve an **overall conversion rate increase of between 2% and 5%.**
- These companies typically see their **revenue per visitor jump by between 5% and 7%.**
- After starting to work with Namogoo, these companies see a **90% reduction in the online revenue being lost** to ad injections.
- Among these companies' "infected" customers (customers who were actively targeted by ad injectors) in the first half of 2019, **those whose injected ads were blocked by our CHP solution typically converted at a rate 48.98% higher than those whose injected ads were not blocked.**
- To date, our CHP solution has enabled these companies to **recover a total of over $650 million** that would otherwise be lost to ad injections.

One retailer taking on client-side threats through our Customer Hijacking Prevention solution is the iconic subscription box brand Dollar Shave Club. After realizing what a threat CJH posed to its business model, this enterprise turned to Namogoo to stop injected ads from stealing away its customers. Working with our platform, Dollar Shave Club has improved its customer experience while boosting its overall conversion rate by 4.6%.

"We understood the potential impact to our sales just by seeing how these [injected] ads were pointing our customers to other sites," explains Jason Bosco, Dollar Shave Club's VP of Engineering. "Most customers are not technical enough to understand that these ads were not actually coming from us, and the poor user experience they were causing was harmful to how these customers would perceive our brand."

Just as the bad actors who engage in Customer Journey Hijacking are becoming more sophisticated, so are the tools available to retailers looking to protect their eCommerce investments. With such advanced technologies at their disposal, today there is really no reason these companies need to let themselves fall victim to CJH.

That leaves ad injectors with one major asset enabling them to continue their methods of Customer Journey Hijacking: Many retailers are still unaware of the client-side threats facing their businesses and of the high-tech solutions available to them today.

Conclusion

Today's retailers know that eCommerce success depends on offering a high-quality online experience to their customers and prospective customers. That's why they invest so heavily in optimizing their online stores and bringing in traffic from other sources, such as paid advertisements and organic social media content.

But as they devote such significant resources to fostering sales, brand reputations, and long-term customer relationships through their online assets, many retailers are not yet aware of the full power of the client-side threats that undermine their investments through Customer Journey Hijacking.

Meanwhile, CJH is a particularly difficult problem to solve, because conventional cybersecurity solutions cannot prevent client-side malware or Wi-Fi hijacking from causing injected ads to appear on a user's device.

Still, AI-driven technological advances have made it possible to take on ad injectors through intelligent Customer Hijacking Prevention.

As shown by the data we have collected through extensive A/B testing, blocking injected ads in real time enables retailers to boost KPIs such as conversion rate and average revenue per visitor, enabling them to recover fully 90% of the revenue they would otherwise lose to CJH.

In short, while the sophistication of ad injectors continues to increase, so do retailers' abilities to fight these client-side threats through intelligent, real-time tools.

15% to 25% of Your Customers Are Disrupted by Unauthorized Ads

How prevalent is Customer Journey Hijacking within your online store?

Find out how client-side ad injections are affecting your customer experience and your sales revenue.

Get a Free Website Analysis

Namogoo's client-side platform provides full visibility and control to prevent Customer Journey Hijacking and protect user privacy for online enterprises.