NAMOGOO

Customer Journey Hijacking: The Business Partner You Never Knew You Had

Here's How Traffic Hijackers Are Using This Tactic to Skim Your Online Revenue

What is Customer Journey Hijacking?

Customer Journey Hijacking is a widespread problem whereby unauthorized ads are injected into consumer devices and web browsers. Once running, these ad injections appear to online visitors throughout the eCommerce site, disrupting their online shopping journey and diverting them to other sites. These ad injections include:

- Product ads and recommendations
- Pop-ups
- Banners
- UI hijacking, including in-text and inline redirects targeting text, links, and buttons

The majority of these ads promote competitor websites and similar product offerings. Customer Journey Hijacking is not sanctioned by the user, or by the website.

What is ad injection?

Ad injection is a technique that inserts advertisements into web pages without the site owner's consent. Ad injections are intended to get online consumers to click on them and redirect them to other sites.

While there are many types of injections used by 3rd parties to exploit consumer devices and web browsers, ad injection is specifically used by traffic hijackers to monetize web traffic by selling ad impressions and clicks to ad networks.

How do online customers get hijacked?

In order to inject ads that enterprises can't detect, traffic hijackers need access to the consumer's device. They get this access using 4 main techniques:

1. Developing and distributing supposedly legitimate, and in most case free software services that add value to the consumer, such as:
   - Desktop software
   - Browser extensions
   - Mobile apps
2. Incentivizing other legitimate software services to bundle in their ad injectors via installation wizards, paying a commission every time a user downloads and installs their software (Pay-per-install).
3. Misleading consumers into downloading popular legitimate software through an alternative, unauthorized source
4. Free public Wi-Fi hotspots (e.g. at cafes, hotels, airports etc.) that monetize their services via ad injections.

Popular free software consumers download include:

- File converters
- Antivirus
- Device performance boosters
- Deals & coupons notifications
- Media players
- Traffic & navigation

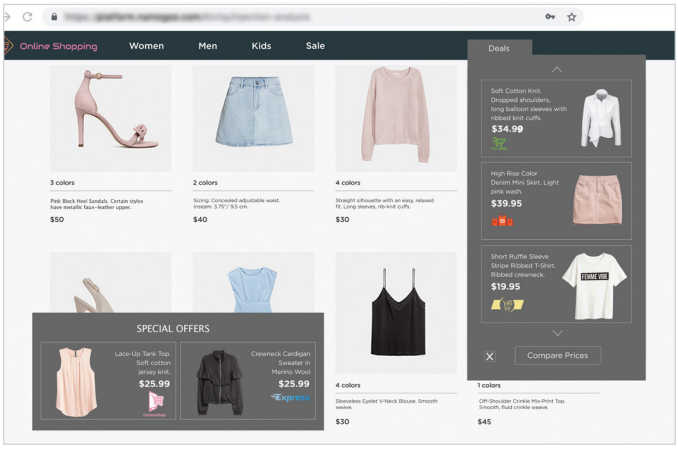
Who are traffic hijackers?

Traffic hijackers are companies that use ad injection to profit from traffic monetization on websites they don't own and are not in partnership with.

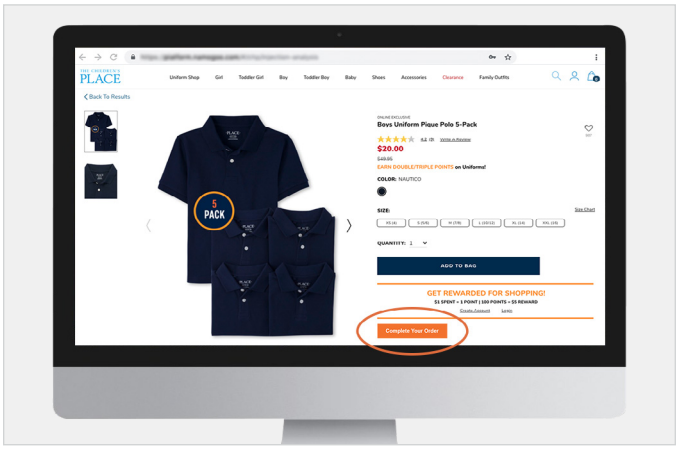
They sometimes position themselves as traffic monetization solutions, offering free software developers a way to monetize their services.

What do ad injections look like?

Overlays / pop-ups recommending offers from other sites:



UI hijacking a button on a product page:



What is the scale of the problem? How many online customers are hijacked?

Namogoo analyzes more than 20 billion pageviews per week for over 250 of the largest online brands in the world. Across all industries, our data shows that between 15 and 25% of all website visitors are hijacked throughout the year. The lowest hijacking rate recorded so far is 11.5%.

Why have I never seen ad injections in any of my session recording play-throughs?

Since the injection is happening locally on the consumer's device, often delivered via iframes, it is impossible for you to view content injected entirely on the user's browser or device, outside of data exploration. Data may indicate that 1 in 5 of your visitors act differently than everyone else. Without the prior knowledge that these visitors are hijacked, it would be very difficult to detect the same.

Our servers are encrypted — how is my site being hijacked?

While you do a tremendous job of hardening your servers and your CDNs, once your website is rendered on the end user's device, the control is out of your hands.

What's the business impact of preventing Customer Journey Hijacking?

Eliminating consumer-side ad injections and the disruptions they cause to the online customer journey immediately impacts eCommerce revenue. Enterprises preventing Customer Journey Hijacking with Namogoo's solution are consistently improving these online KPIs:

1.5-5%
Increase in
Conversion Rate

5-9%
Decrease in Checkout
Abandonment Rate

5-7%
Increase in
Revenue Per Visitor

Find out how many of your site visitors are disrupted by Customer Journey Hijacking and the impact on your revenue.

Request a Demo **Contact Us**

About Namogoo

Namogoo is pioneering the market of Customer Journey Hijacking Prevention. The company's disruptive technology protects the customer journey for online enterprises by identifying and blocking unauthorized product ads injected into consumer browsers that divert site visitors to competitors and hurt conversion rates. The world's largest retailers rely on Namogoo to deliver a disruption-free customer experience and consistently increase eCommerce revenue.