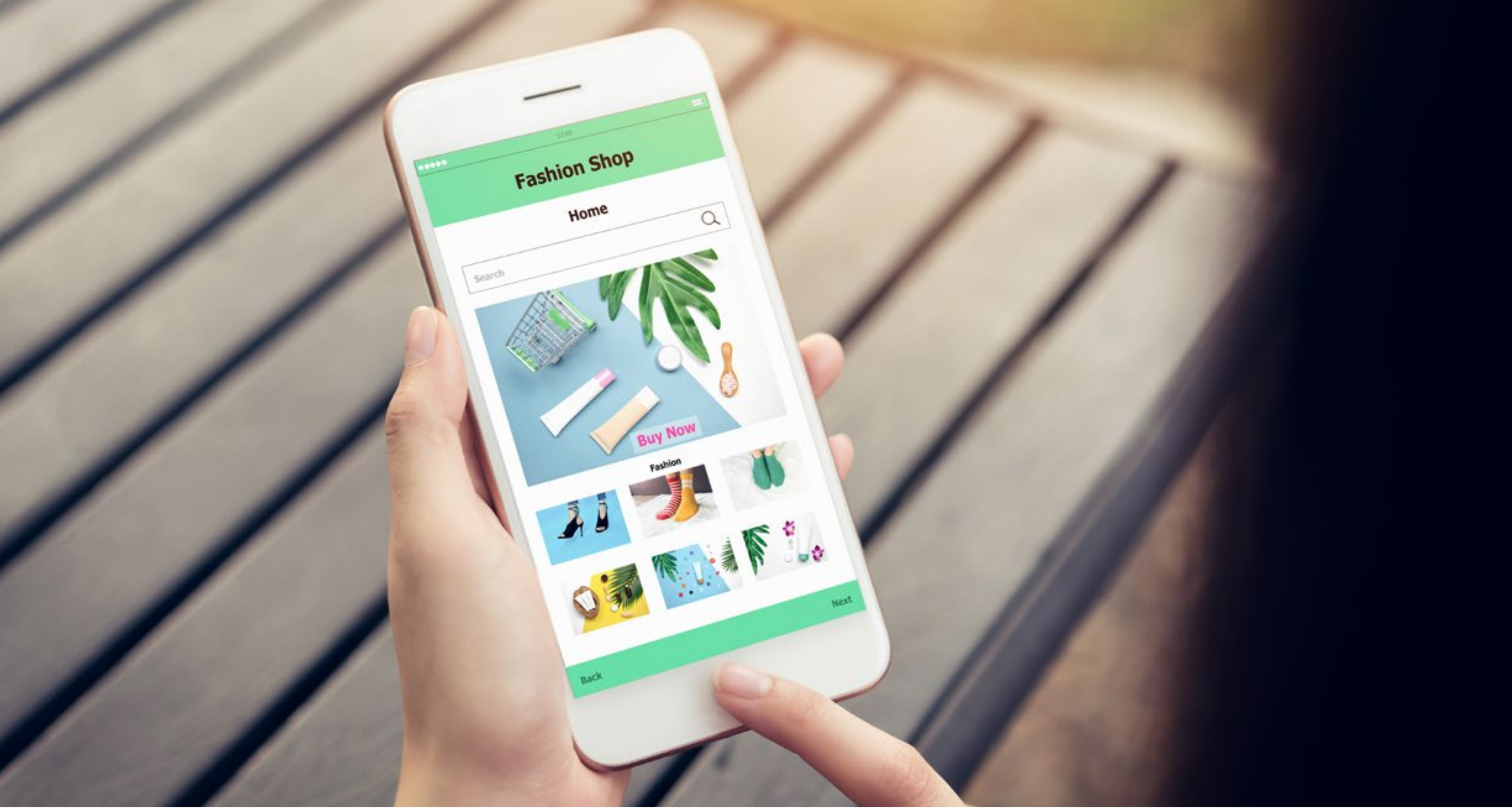
AD INJECTORS AND CUSTOMER JOURNEY HIJACKING: THE REVENUE LEAKAGE YOU DIDN'T KNOW YOU HAD!

Abstract

Seemingly harmless browser extensions, public wifi, plug ins and apps can be host to ad injectors that display illegitimate ads. These illegitimate ads can interrupt browsing sessions and divert users to competitor sites resulting in Customer Journey Hijacking. Customer Journey Hijacking not only affects customer experience but can also lead to online revenue leakage. Creating awareness around customer journey hijacking and the efficient use of AI/ML solutions is the only way forward to plug this leak.

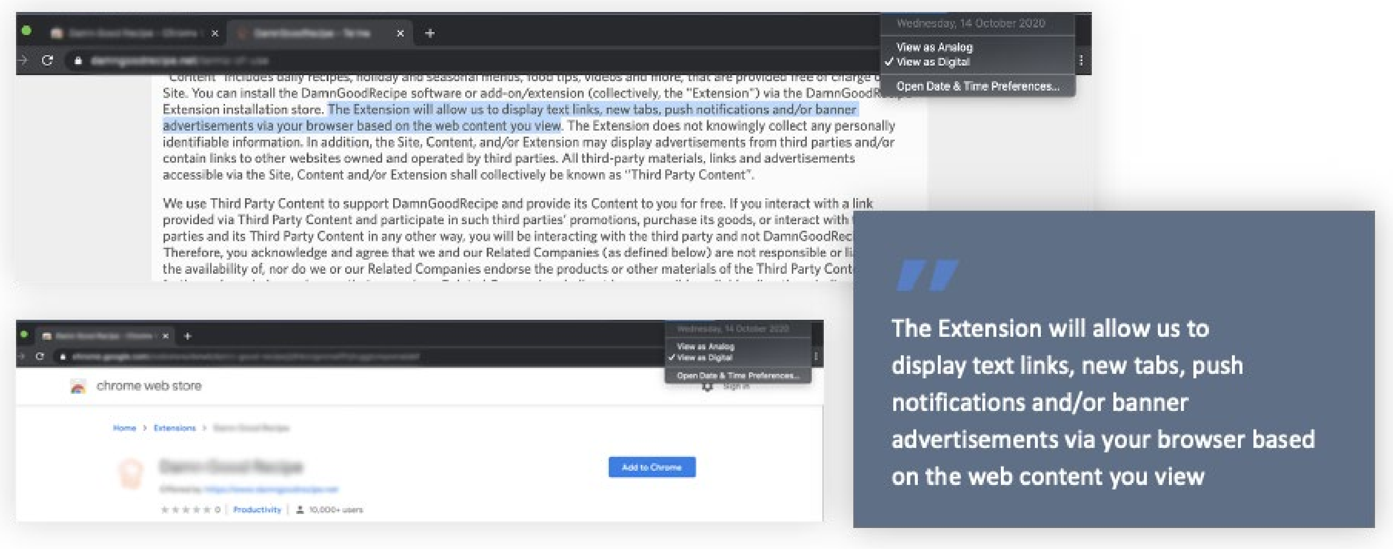
NAMOGOO

Infosys®
Navigate your next



Ecommerce sites are precious real estate for any brand as they leverage it to sell their products and avail additional revenue through online advertising (Cost per Acquisition (CPA), Cost per Mille (CPM), and Cost per Click (CPC)). However, analysis of customer session data of over 250 online retail brands shows that 20% of all online shopping sessions are exposed to unauthorized ad injections. These unsanctioned promotions not only divert revenue away from the websites they appear on but also divert active customer shopping sessions directly to competitor sites.

Ad injections are illegitimate ads fed through softwares running on the end-user device (ad injectors). These ad injectors are installed when a user downloads browser extensions, plug-ins, apps, or even while connecting to a public WiFi network. However, the user is often oblivious of these installations and their capability to inject ads. Ad injectors surreptitiously monitor all web activities, superimpose ads during web sessions, and thereby deteriorate customer experience and web monetization.



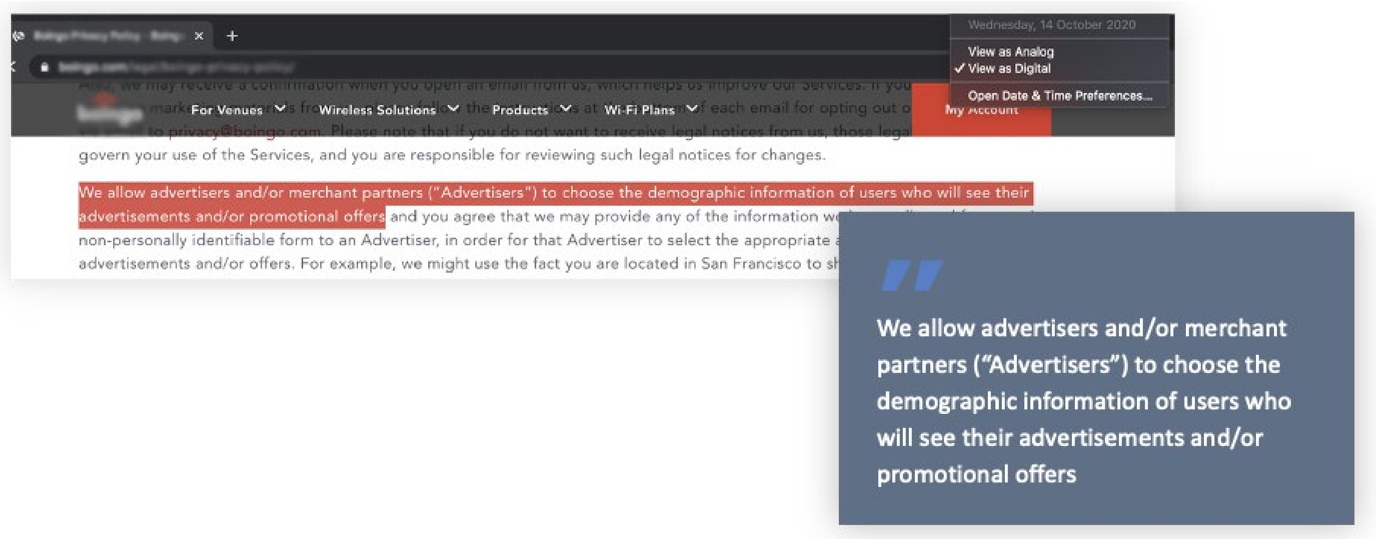
"Content" includes daily recipes, holiday and seasonal menus, food tips, videos and more, that are provided free of charge o
Site. You can install the DamnGoodRecipe software or add-on/extension (collectively, the "Extension") via the DamnGoodR
Extension installation store. The Extension will allow us to display text links, new tabs, push notifications and/or banner advertisements via your browser based on the web content you view. The Extension does not knowingly collect any personally identifiable information. In addition, the Site, Content, and/or Extension may display advertisements from third parties and/or contain links to other websites owned and operated by third parties. All third-party materials, links and advertisements accessible via the Site, Content and/or Extension shall collectively be known as "Third Party Content".

We use Third Party Content to support DamnGoodRecipe and provide its Content to you for free. If you interact with a link
provided via Third Party Content and participate in such third parties' promotions, purchase its goods, or interact with t
parties and its Third Party Content in any other way, you will be interacting with the third party and not DamnGoodRec
Therefore, you acknowledge and agree that we and our Related Companies (as defined below) are not responsible or li
the availability of, nor do we or our Related Companies endorse the products or other materials of the Third Party Cont

Wednesday, 14 October 2020
View as Analog
✓ View as Digital
Open Date & Time Preferences...
chrome web store
Home > Extensions >
Add to Chrome
★★★★★ 0 | Productivity | 10,000+ users

> The Extension will allow us to display text links, new tabs, push notifications and/or banner advertisements via your browser based on the web content you view

Browser Extensions: Permission declaration & warning before adding browser extensions



... to privacy@boingo.com. Please note that if you do not want to receive legal notices from us, those lega... govern your use of the Services, and you are responsible for reviewing such legal notices for changes.

We allow advertisers and/or merchant partners ("Advertisers") to choose the demographic information of users who will see their advertisements and/or promotional offers and you agree that we may provide any of the information w... non-personally identifiable form to an Advertiser, in order for that Advertiser to select the appropriate a... advertisements and/or offers. For example, we might use the fact you are located in San Francisco to sh...

> We allow advertisers and/or merchant partners ("Advertisers") to choose the demographic information of users who will see their advertisements and/or promotional offers

Public Wifi monetizing users: User agreement terms

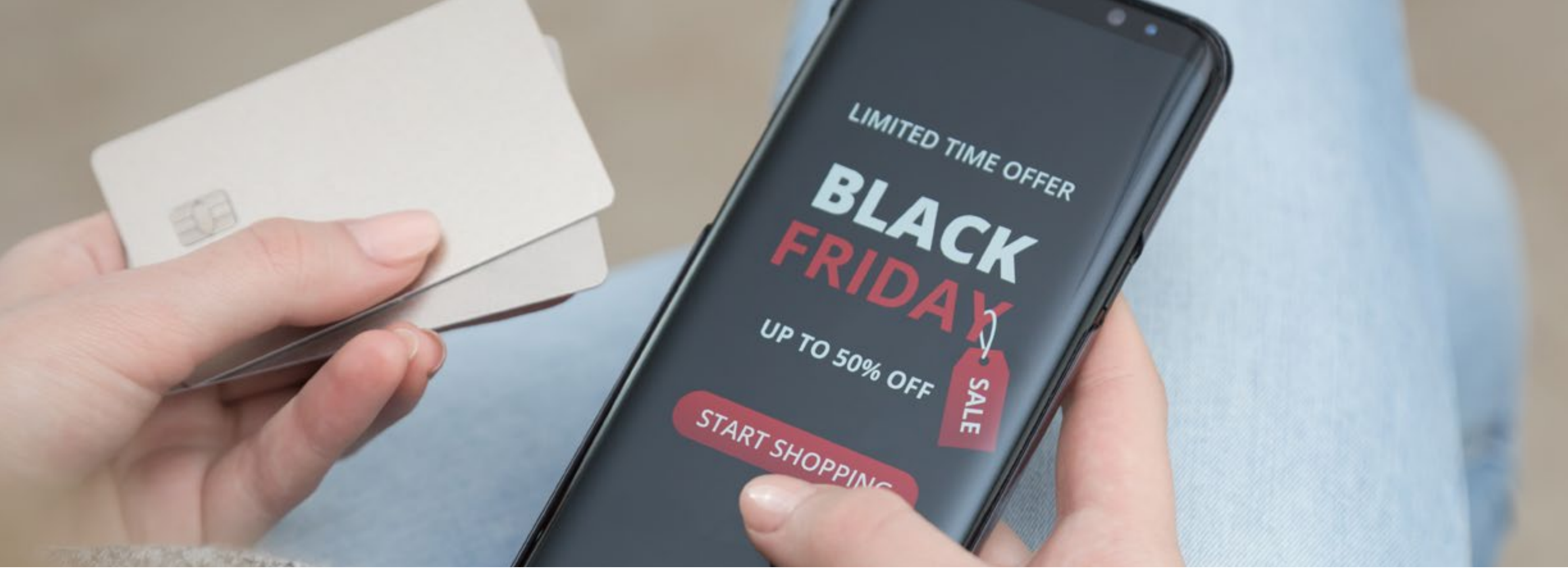
Ad Injectors and Customer Journey Hijacking

Traditionally, brands monetize their websites (publishers) by selling advertisement spaces on ad exchanges or ad networks. While ad networks sell impressions for a marked-up price, ad exchanges conduct auctions and award impressions to the highest bidder in real-time. The entire process of an impression auction takes place in milliseconds, the time it takes for the consumer's device to load a page.

Ad injectors act like publishers in the traditional advertising ecosystem by sourcing ads from advertising exchanges and covertly displaying them on a webpage. These ad injections might appear above the legitimate ads the webpage page displays or might even take up a space that was never auctioned. The event where customers fall pray to these illegitimate ads and are diverted to another website is known as Customer Journey Hijacking. Customer Journey Hijacking not only affects the online revenue but also the customer experience and brand reputation as customers are being redirected to a competitor or disreputable site.

Websites and brands are oblivious to these hijacks as the source of the ads cannot be monitored or controlled by the page owner. In this scenario, the genuine website publisher loses on web monetization and brand reputation while the ad injectors, ad networks and advertisers profit from the CPM, CPA and CPC metrics.

A study conducted in 2015 found that 5.5% of unique daily IP addresses visiting Google properties have at least one ad injector installed (Thomas, et al., 2015). The same study observed that ad injectors profit from over 3000 advertisers including Sears, Walmart, eBay, and Target. Just like the affected websites, these advertisers are also oblivious to the traffic from ad injectors because their visibility is limited to the last intermediary in a very complex web of intermediaries. Its solution lies in general awareness around Customer Journey Hijacking and a sophisticated tool to detect and prevent ad injectors at the right time and journey point.



Downside for both Publishers and Advertisers

It goes without saying that publishers are suffering at the hands of ad injectors. Ad injectors monitor all of the consumer's browser activity including page interactions and search queries and pass it on to third parties for advertisement selection. This process not only impacts the consumer's security and privacy but also increases page load latency. When a browsing session is affected by ad injectors, a completely different user experience emerges. The publisher's page will be inundated with unrelated and spurious ads that engulf the original content. These ads could even mimic the page style, tricking the site visitor into clicking, eventually hijacking their journey by leading them to a competitor or objectionable site. In addition to a lost customer, the ads give the consumer the impression that the website is at fault, thereby potentially degrading the brand reputation.

Here, brand reputation is at stake not only for the publishers but also for the advertisers as their ads can be displayed on any site from competitors to ones with contentious content. Since the advertisers are oblivious to the provenance of their traffic, they are tricked into believing that a genuine affiliate or publisher is being benefitted.

The lack of awareness on ad injection and the millions of dollars lost to Customer Journey Hijacking is one of the major challenges in tackling the ad injection problem. Google's public announcement and acceptance of the problem, displaying warnings before downloading sketchy extensions, and its work on Unwanted Software Policy are a few steps to mitigate ad fraud. However, policies and warnings can only manage this increasing problem to a certain extent.

The Fight against Ad Injectors and Customer Journey Hijacking

More than tens of thousands of ad injections are detected weekly, hence manual blacklisting is immensely time-consuming and insufficient. In addition to the sheer volume of these injections, the constant updating of scripts to evade detection and the daily upload of new apps and extensions on app stores make it increasingly difficult to effectively detect and prevent ad injections.

To stay ahead of this volume and variety game in ad injections, companies require efficient machine learning capabilities. Preventing Customer Journey Hijacking and the impact that client-side ad injections have on the online customer experience and bottom-line KPIs for eCommerce brands, demands technology that is both dynamic and continuously self-learning. This Customer Journey Hijacking prevention capability should be able to identify and classify illegitimate activities, scripts, domains, IPs, iFrames, and other elements running on the customer's browser or device and in real-time, prevent their execution before page rendering.

However, this is a complex and resource-intensive task considering the origin and complexity of ad injections. Since ad injectors use multiple methods (desktop software, browser extensions, apps, plugins) that allow them to inject ads into the consumer's browser, they cannot be detected by server-side solutions. Therefore, leveraging emerging innovations that can provide comprehensive coverage of all these client-side factors and their impact on each customer's experience is the only solution to help online enterprises. Such a solution will not only ensure a disruption-free customer experience but also allow enterprises to prevent revenue leakage, protect brand reputation, and enforce customer retention.

Our Take

We understand the criticality of Customer Journey Hijacking and similar business problems and the need to prevent them before they onset. Hence, through the Infosys Innovation Network (IIN), we work with startups in our Innovation Ecosystem to not only identify solutions but also create awareness around these business issues.

Namogoo, one of the Infosys Innovation Network (IIN) partner startups, has been in Customer Journey Hijacking prevention since 2014. Namogoo's platform prevents customer journey hijacking by identifying unauthorized ad injections and blocking them. Namogoo analyses over 500 million web sessions weekly and its Machine Learning powered solution helps brands improve visibility, efficiency, and governance of their web ecosystem. Leveraging our partnership with Namogoo, we are educating clients and helping them improve their online revenue. With opportunities across industries like travel, publishing, retail, and hospitality, Namogoo aims to establish itself as a necessary provider for all e-commerce brands. As brands catch up with the awareness on ad injectors and associated online revenue loss, Namogoo is set to become the leading player in the prevention of customer journey hijacking.

Case Study

Problem Statement: Customers browsing the fast-fashion retailer New Look's site were exposed to ads from direct competitors, and ads that were irrelevant to the shopping resulting in revenue loss and bad customer experience.

Solution: Following the successful 30-day proof of value implementation with New Look, Namogoo implemented its platform to ensure a distraction-free browsing experience.

Impact: In the quarter following Namogoo implementation, New Look's conversion rate rose by 3.8 percent while revenue per visitor increased 3.5 percent.

Bibliography

- BILTON, R. (2015, May 11). WTF is Ad Injection? Retrieved from DigiDay: https://digiday.com/media/wtf-ad-injection/
- Chowdhry, A. (2018, March 26). How Namogoo Is Preventing 'Online Journey Hijacking' For Top E-Commerce Brands. Retrieved from Forbes: https://www.forbes.com/sites/amitchowdhry/2018/03/26/namogoo/?sh=6b722eb468f3
- Johnsen, V. (2015, September 10). Cutting Unwanted Ad Injectors Out of Advertising. Retrieved from Google Blog: https://security.googleblog.com/2015/09/cutting-unwanted-ad-injectors-out-of.html
- Kahn, R. (2016, April 25). Fighting Ad Injection: What You Need to Know. Retrieved from Ezanga: https://www.ezanga.com/blog/fighting-ad-injection-what-you-need-to-know
- Microsoft. (n.d.). Namogoo Customer Journey Hijacking Prevention. Retrieved from Appsource Microsoft: https://appsource.microsoft.com/en-us/product/web-apps/namogoo1592241042558.namogoo_chp_us_1?src=manufacturing&tab=Overview
- Thomas, K., Bursztein, E., Grier, C., Ho, G., Jagpal, N., Kapravelos, A., . . . Rajab, M. A. (2015). Ad Injection at Scale: Assessing Deceptive Advertisement Modifications. Retrieved 11 5, 2020, from https://research.google/pubs/pub43346

About iCETS

The incubation center of Infosys called 'Infosys Center for Emerging Technology Solutions' (iCETS) focuses on incubation of NextGen services and offerings by identifying and building technology capabilities to accelerate innovation. The current areas of incubation include AI & ML, Blockchain, Computer Vision, Conversational interfaces, AR-VR, Deep Learning, Advanced Analytics using video, speech, text and much more.

About IIN

The Infosys Innovation Network (IIN) is a well-orchestrated partnership between select startups and Infosys to provide innovative services to our clients. The IIN program aims to create lighthouse wins for clients to experiment and implement art-of-the-possible. Infosys de-risks client adoption of technology products & solutions by carefully curating these startups, finding the right fit and implementing early pilots.

About Namogoo

Namogoo has revolutionized the online customer journey with innovative technology, becoming a market leader. Their Digital Journey Continuity platform drives the customer journey forward for over 150 global online brands. Namogoo's disruptive technology incorporates patented data points, consumer-side signals, behavioral analytics, and prediction algorithms to autonomously adapt every journey to each individual customer, clearing the path to purchase and perfectly positioning them to reach their destination.

Authors

Anu Mary Tom

Anu Mary Tom is a Senior Associate Consultant at Infosys Center for Emerging Technology Solutions. She has significant experience across Digital Experience and Emerging Technologies and is currently involved in GTM, research and partnership activities at Infosys.

To know more about the Infosys Innovation Network (IIN), Namogoo, and how we can help you drive customer journeys, please reach out to iCETS@infosys.com.

For more information, contact askus@infosys.com

Infosys®
Navigate your next