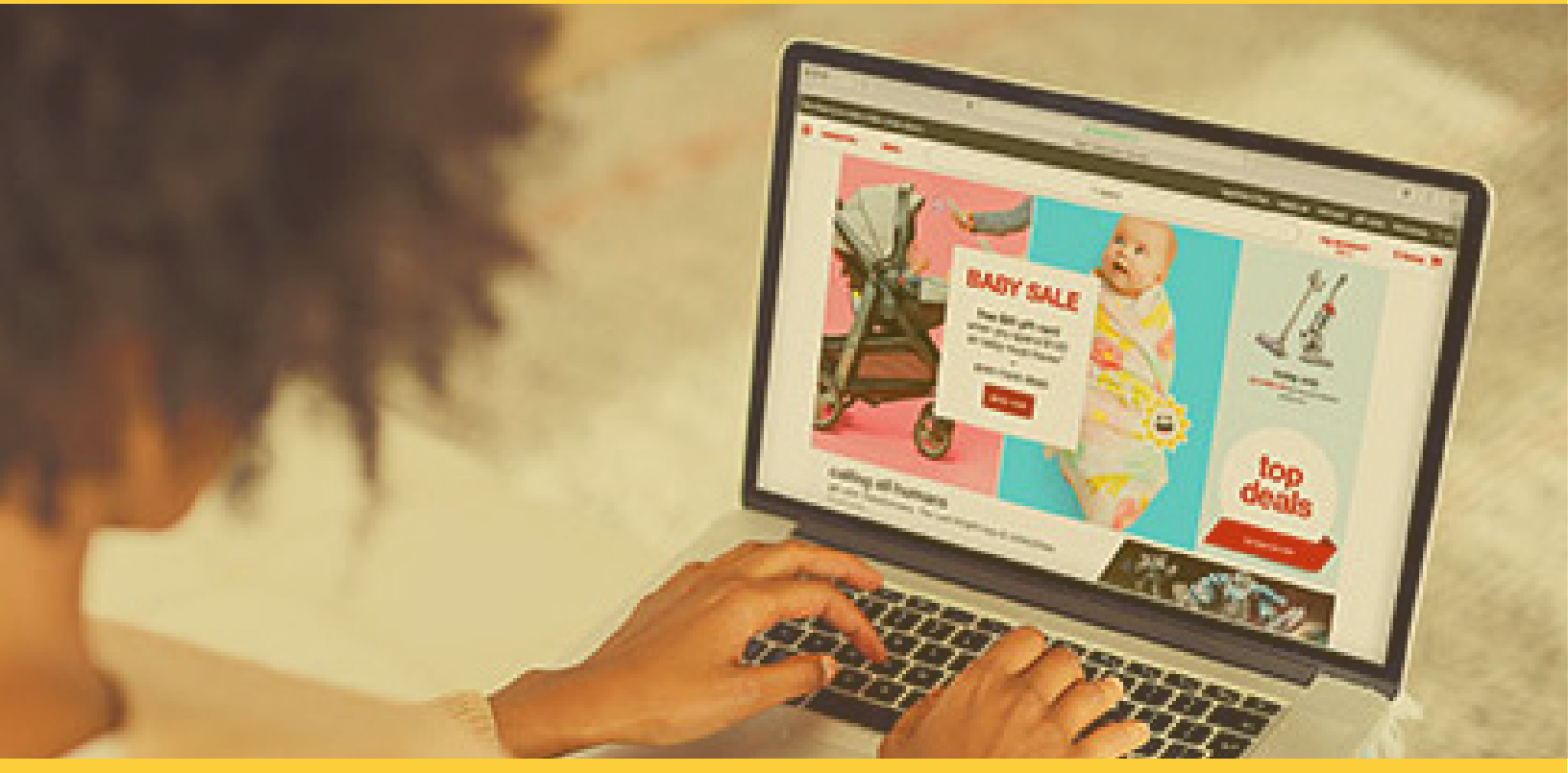
Customer Journey Hijacking Prevention

INCREASE CONVERSION RATES BY ENSURING YOUR CUSTOMERS EXPERIENCE YOUR E-COMMERCE SITE THE WAY YOU INTENDED.



NAMOGOO

PREVENTING JOURNEY HIJACKING

As an owner of your company's e-commerce platform and operations, you invest significant resources in optimizing your online sales, business metrics and customer journey. You understand your potential buyers and their interests, and you have designed the customer experience to meet their needs and expectations. You build and test every page meticulously to maximize results. Now it's just a matter of driving traffic and you're on the road to success, right?

But there's a problem: a significant number of your website customers (15% up to as many as 30% in peak seasons) don't experience your journey as you intended. They encounter a barrage of pop-ups, banner ads, competitor product recommendations and other unwanted distractions. This is caused by client-side Digital Malware running on your customers' browsers and devices, or pushed through Wi-Fi networks, so you have no visibility into this, and no control.

This damaging phenomenon is known as "Customer Journey Hijacking" and its impact on revenue for e-commerce, marketplace and other websites is increasing as you read this. This white paper is intended to help e-commerce companies understand the scope and nature of this problem, show them how they can protect the journey all the way to the browser and win back the lost revenue caused by the customer journey hijack.

What Is Customer Journey Hijacking?

Journey Hijacking is a hidden marketplace that has a massive impact on the online economy. Unauthorized product ads are competing with your business, distracting prospects from your offerings, and cutting directly into your revenue. On top of all this, your customer experience is harmed by the unsavory content littered across your site.

The programs that cause injections are usually bundled in with 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 surreptitiously install themselves via public Wi-Fi connections. All of this happens without your customer even noticing. Infection happens 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 a program has infected a browser, it injects unauthorized widgets (product recommendations and deals), advertisements and spyware scripts. The customer's view of website pages they visit is now

THE SCALE OF THE PROBLEM

Infection rate of Digital Threats

15-30%

Injections that are competitive product ads luring traffic way from the site

40-60%

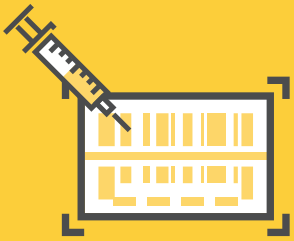
Browser bots running on the application & skewing analytics

3-7%

THE FACE OF A HIJACKED CUSTOMER SITE EXPERIENCE

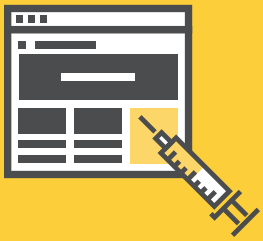
Unauthorized ads designed and injected to lure users away

TO ILLUSTRATE, THE FOLLOWING EXAMPLES OF DIFFERENT TYPES OF INJECTIONS:



INJECTED COMPETITOR PRODUCTS

The web page view is injected with competitor offerings, targeted based on the visitor's intent and context (if they are shopping for a red sweater, they will see competitive offers for red sweaters and related items). The visitor is distracted from what you intended him/her to see, and diverted when they click on the injected products taking traffic and revenue away from your site.



INJECTED ADS

The web page is manipulated to display disruptive banner ads that diminish the site's brand. Inappropriate ads on your site may annoy visitors, compromise your reputation, and harm your visitor retention.

SPYWARE SCRIPTS

Websites are injected with spyware scripts, such as email grabbers and fake surveys, designed to steal email addresses, passwords and otherpersonal information. Fake surveys collect confidential data about the site's visitors, who believe they are sharing their information with a trusted site, exposing your company to serious legal risk. This can result in liability and reputation damage due to stolen visitor details and privacy breaches.

far different from what was intended, filled with 3rd party ads that the website owner did not agree to or receive payment for. That 3rd party is now acting as a "hawker," making money via clicks on the unauthorized ads, selling competitive products, and drawing affiliate fees directing users right back to the original website.

The Impact of Journey Hijacking on Your Business

A huge part of the problem of Journey Hijacking is that neither the e-commerce companies nor their customers are aware that it is happening. Injections look like a native component of a website, so customers have a high propensity to click.

Journey Hijacking through Digital Malware is much more than a nuisance. It has a direct and serious impact on your bottom line. Customers unwittingly click injected ads or banners and you've immediately lost their visit and the related potential revenue. Your analytics are now distorted, too, as you only see that hijacked journey as part of your bounce rate or cart abandonment. On top of that, the trust you've invested so much to build, is now undermined and customer loyalty, already a challenge for online companies, is hurt.

An additional layer of potential damage is that your website privacy terms could be in breach as client-side malware places cookies in your customers' browsers, sometimes falsely under your company's name.

Digital Malware also compromises the security and privacy of your customers' information, including their email address, and exposes them to spam and phishing campaigns.

In terms of quantifying business impact, it is important to understand the prevalence of infection among visitors to e-commerce sites. According to a recent study conducted by Google on the ad injectors

ecosystem, more than 5% of people visiting Google sites have at least one ad injector installed. Of these, 34% of Chrome extensions were defined as outright malware.

Google admitted this is the #1 complaint reported by their sites' visitors. Namogoo believes that actual infection rates are about four times this amount — many of the injection networks were missing in the study. Based on our work with several leading retailers, we have found that between 15-30% of e-commerce site customers are infected. We also found that 40%-60% of the infections done are competitive products.

Why the Current Solutions You're Using Are Not Enough

In most e-commerce companies, the server side of the business operation is tightly protected by a slew of security solutions – from network and application firewalls to SSL and identity management systems.

However, when it comes to the "last mile" (i.e., the visitor's computers and devices), outside of the servers, companies have no control over the security of client-side devices and no visibility into what their visitors actually see when they access the site. Your visitors' devices are in essence the "front door" to your website. If malware gets through the front door via digital malware, all of the server side protection and visibility tools you have doesn't help – the journey gets hijacked and you lose business and visitors. Your current session-simulation and analytics tools can't track this activity so you have no way of understanding how key metrics such as bounce rate and conversion are being distorted.

There is little e-commerce companies can do to secure the client side, other than encouraging their visitors to install anti-malware solutions. In any case, most of these anti-malware tools are not particularly effective against sophisticated injectors that frequently change their signatures. To make matters worse, according to a recent OPSWAT report, over 90% of client devices with an anti-virus engine installed had not run a full scan in the last seven days, putting them at risk for infection. Ironically, a number of the popular free anti-virus tools are also often bundled with malware that injects ads.

COMPANIES RECOUP AN AVERAGE

1-5%

OF 1-5% OF ONLINE REVENUE BY BLOCKING

INJECTED CONTENT—TRANSLATING

TO TENS OF MILLIONS OF DOLLARS.

Typical Digital Malware Infection Scenario

The following is a typical scenario illustrating how an innocent visitor gets infected with client-side malware and then sees ad injections on an e-commerce site:

01 Developers create an extension for injection on a browser
02 Third party platforms are used to bundle the extension or app with legitimate software based on a revenue sharing model
03 The innocent customer downloads an extension or app (such as free video player) with a bundled injector
04 The customer goes to an e-commerce site
05 The web page is served from the web server as it should correctly appear
06 Immediately after the page renders, the Digital Malware on the customer's browser injects content into empty spaces or overrides existing content. Depending on its sophistication, the injection may or may not be apparent to the visitor.

The New Way to Prevent Online Journey Hijacking

Namogoo offers end-to-end prevention of any type of injected malware (e.g. adware, spyware scripts, widgets) that affects your customers' browsing experience and hijack the online journey. The Namogoo solution was built with a single goal in mind – to make sure your website is viewed exactly as you intended, every time and by every customer. By blocking client-side malware before it impacts your the visit, Namogoo guards the journey all the way to the browser and prevents lost revenue, brand abuse and privacy infringement.

Namogoo's servers scan hundreds of millions of pages daily, generating hundreds of thousands of malware injection patterns in real-time and applying them to your sessions via a single line of code. Namogoo recognizes injection patterns and blocks them, so the customer's browser only renders legitimate and authentic elements of your website. Patent-pending Machine Learning technology enables real-time detection and elimination of injected malware — while keeping a zero rate of false positives — an essential requirement in e-commerce environment

Namogoo's technology was designed to be integrated with zero-effort and development resources on the merchant side. By adding a single line of JavaScript code that communicates asynchronously with an advanced back-end system, the service can be added within a few minutes to deliver immediate results.

An intuitive and convenient tracking and monitoring dashboard allows e-commerce companies to view up-to-the-minute information on identified injections, anonymous visitor-related data and impact estimates.

Namogoo's advanced technologies are uniquely designed to meet the needs of today's e-commerce companies:

INHERENT SCALABILITY

Namogoo is built to deliver high performance for sites of any size. A robust, scalable and fault-tolerant architecture is designed to handle billions of pages per month with high capacity storage. The system has been implemented for a number of very large retailers with excellent results.

SELF-LEARNING PROTECTION

Advanced machine learning algorithms identify changes in injection fingerprints and automatically adapt the security rules so your protection is always up to date.

ZERO-EFFORT DEPLOYMENT

Namogoo supports all types of website platforms. With our zero integration SaaS solution — simply drop a line of code in your website and you're up and running.

SEAMLESS INTEGRATION INTO ANY ANALYTICS PLATFORM

Namogoo sends real-time events into any analytics platform and solution, adding Namogoo's proprietary data points into the existing data warehouse.

WHEN USING A SOLUTION THAT PROVIDES GRANULAR INSIGHT INTO WHAT IS BEING PREVENTED, COMPANIES CAN EASILY MEASURE BUSINESS BENEFITS.

Increase conversion rates of infected population by 10%–20% by eliminating injected ads and banners that divert visitors to third-party "hawker" sites.

Reduce shopping cart abandonment of infected rate of population by 20%–40%.

Eliminate privacy infringements related to spyware injections.

Decrease in Bounce Rate within infected population by 10%-17%.

Enhance customer retention rate of infected population by 15%-20% by ensuring a flawless and intentional customer experience.

Increase session length per customer of infected population by 15%-20%.

Reduce page loading times of infected population by 10%-15%.

Preserve brand reputation by keeping inappropriate ads off your site.

Leading e-Commerce Brands are Already Taking Action

Online businesses are opening their eyes to the extent that Journey Hijacking is impacting their business. Preventing client-side injected ads and protecting the customers' journey leads directly to higher e-commerce revenues and increased visitor retention and customer loyalty.

In Summary

Client-side Digital Malware that hijacks the online journey is a real and growing threat to e-commerce businesses and is only expected to continue to grow. It adversely affects the user experience and "skims" serious revenues from websites.

However, since Digital Malware affects the customer's browser rather than the web server, it is basically invisible to website owners. Particularly in large organizations, it is virtually impossible to identify customers that are "lost" to clicks on injected products and banners.

The first step in fixing this problem is raising awareness among stakeholders within your organization that the threat exists, as well as recognizing the magnitude of its business impact. It is also important to understand that your current security solutions cannot, and were not designed to, prevent this type of threat, and that a specific solution is necessary.

Namogoo's technology fills what was previously a void in the market, providing e-commerce sites with a simple-to-deploy, end-to-end solution for handling Digital Malware threats.

BENCHMARK RESULTS OF INFECTED AUDIENCE

SALES FUNNEL IMPROVEMENT

- **15–20%** Increase in retention rate
- **5–7%** Decrease in cart abandonment
- **10–17%** Increase in conversion

CUSTOMER EXPERIENCE IMPROVEMENT

- **10–17%** Decrease in bounce rate
- **15–20%** Increase in number of sessions per customer
- **10–15%** Reduction in page load performance

If you'd like to learn more about how Namogoo can protect your customers from client-side injected ads and get a free analysis of how infected visits are currently infecting your website, please contact us:

info@namogoo.com / 857.284.8084.

BOSTON
745 Atlantic Ave
Boston, MA 02111
USA

ISRAEL
7 HaSadna St.
Ra'anana 4365004
Israel

NAMOGOO

namogoo.com 857.284.8084