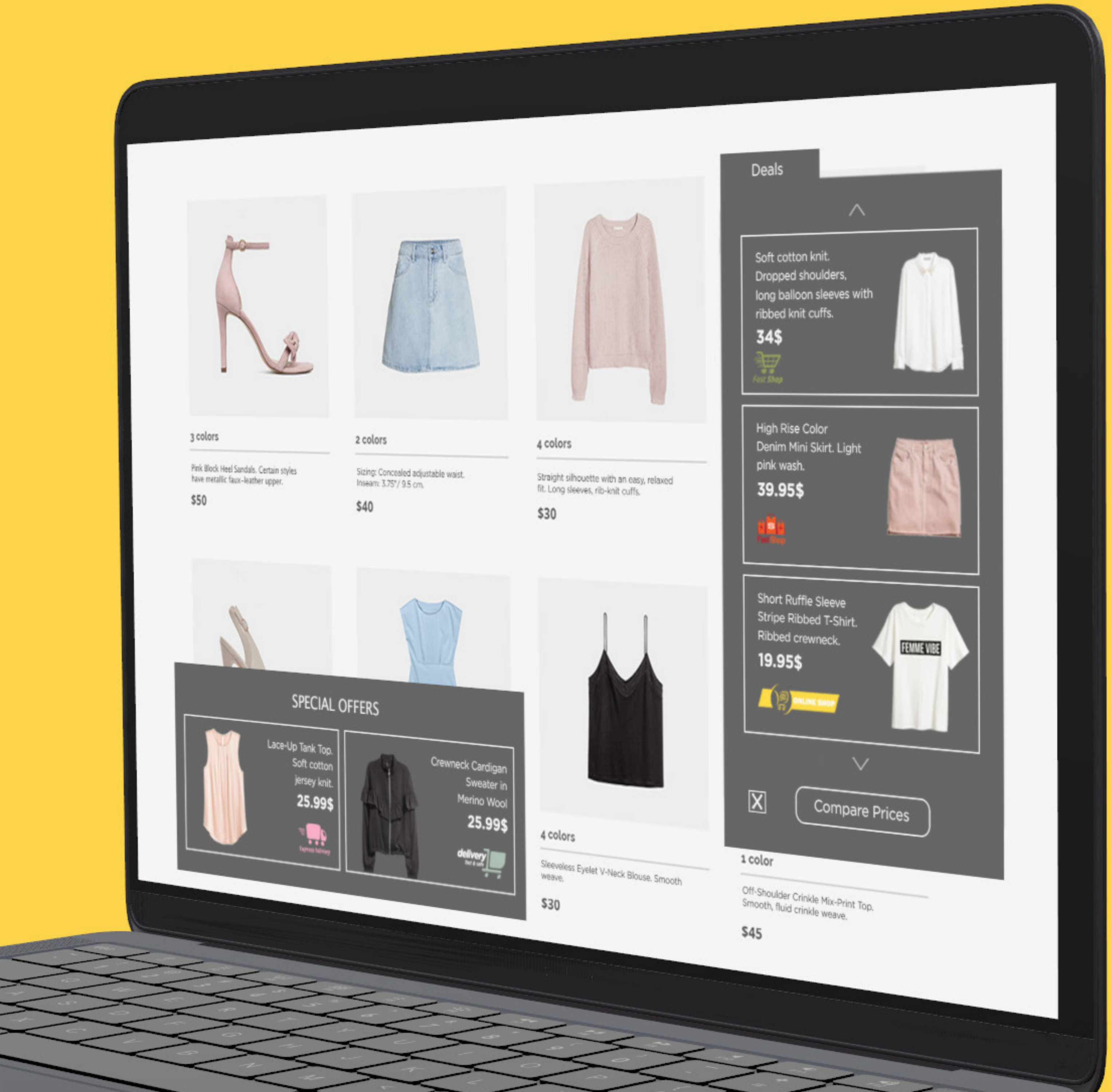
NAMOGOO

2019 REPORT

THE STATE OF ONLINE JOURNEY HIJACKING 2018



Deals

Soft cotton knit. Dropped shoulders, long balloon sleeves with ribbed knit cuffs.

34$

Fast Shop

High Rise Color Denim Mini Skirt. Light pink wash.

39.95$

Short Ruffle Sleeve Stripe Ribbed T-Shirt. Ribbed crewneck.

19.95$

ONLINE SHOP

X

Compare Prices

3 colors

Pink Block Heel Sandals. Certain styles have metallic faux-leather upper.

$50

2 colors

Sizing: Concealed adjustable waist. Inseam: 3.75"/ 9.5 cm.

$40

4 colors

Straight silhouette with an easy, relaxed fit. Long sleeves, rib-knit cuffs.

$30

SPECIAL OFFERS

Lace-Up Tank Top. Soft cotton jersey knit.

25.99$

Crewneck Cardigan Sweater in Merino Wool

25.99$

delivery

4 colors

Sleeveless Eyelet V-Neck Blouse. Smooth weave.

$30

1 color

Off-Shoulder Crinkle Mix-Print Top. Smooth, fluid crinkle weave.

$45

About This Report

Online Journey Hijacking, a client-side phenomenon where unauthorized ads are injected into consumer browsers, is a growing yet invisible problem for eCommerce sites. This issue is widespread across the web — yet the eCommerce industry has only been made aware of its existence in recent years.

As the first and only solution to help online businesses eliminate the impact of Online Journey Hijacking, Namogoo is leading the mission to educate the market about the scale and impact of this problem on both user experience and online business revenue.

Findings in this report are based on an analysis of hundreds of millions of page views across verticals, and include exclusive data insights that provide an in-depth look into this phenomenon and how it is affecting online businesses.

Following our H1 2018 benchmark report, the data in this edition provides a complete summary of 2018 by quarter. Data in this report covers both desktop and mobile consumer web sessions in the U.S. and Europe across a variety of verticals.

To ensure industry knowledge of Online Journey Hijacking and awareness of its scale and impact remains at the forefront, this report will be updated biannually with new trends and insights.

The Namogoo Team

About Online Journey Hijacking

What is Online Journey Hijacking?

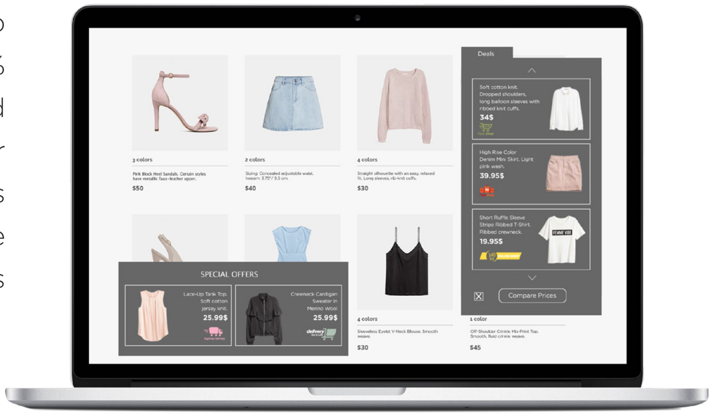
Online Journey Hijacking is a rapidly growing phenomenon where unauthorized ads are injected into consumer browsers. These unsanctioned promotions are injected by digital malware that infects browsers and devices when users install software downloads or program updates, or in other cases, when they connect to public WiFi networks.

Once the digital malware is running on the web browser or device, online consumers are interrupted by injected product ads, pop-ups, banners and in-text redirects when browsing eCommerce sites. Because the malware resides on the user's browser or device, server-side security solutions lack visibility or control over the problem.

The Scale of the Problem

According to a widely referred-to Google report, ad injections impact tens of millions of users globally, and have been cited as the single largest source of frustration among Chrome users.

In the course of analyzing hundreds of millions of web sessions weekly, Namogoo's data shows that 15-25% of all user web sessions are exposed to unauthorized ads. In 40-70% of these cases, the ads feature competitor promotions or products that divert customers to the retailer's competitors. These infections increase substantially during peak shopping seasons such as during the holidays and can exceed 30%.


3 colors
Pink Block Heel Sandals. Certain styles have metallic faux-leather upper.
$50
2 colors
Sizing: Concealed adjustable waist. Inseam: 3.75"/ 9.5 cm.
$40
4 colors
Straight silhouette with an easy, relaxed fit. Long sleeves, rib-knit cuffs.
$30
Deals
Soft cotton knit. Dropped shoulders, long balloon sleeves with ribbed knit cuffs.
34$
High Rise Color Denim Mini Skirt. Light pink wash.
39.95$
Short Ruffle Sleeve Stripe Ribbed T-Shirt. Ribbed crewneck.
19.95$
FEMME VIBE
Compare Prices
SPECIAL OFFERS
Lace-Up Tank Top. Soft cotton jersey knit.
25.99$
Crewneck Cardigan Sweater in Merino Wool
25.99$
delivery
4 colors
Sleeveless Eyelet V-Neck Blouse. Smooth weave.
$30
1 color
Off-Shoulder Crinkle Mix-Print Top. Smooth, fluid crinkle weave.
$45

The Impact to Online Businesses

In the digital commerce arena, any interruptions distracting customers away from the intended online experience hurt the ability for businesses to convert and retain site visitors, and generate revenue. Through various types of injected ads, Online Journey Hijacking disrupts users throughout their journey with invasive promotions that redirect them to competing product offers, cutting directly into eCommerce conversions and revenue.

In Namogoo's 2018 Consumer Behavior Study surveying over 1,300 U.S. online shoppers, over 58% of consumers indicated they were likely to click on product ads offering lower-priced products, while over 77% stated that encountering pop-ups, banners or advertisements from other sites would negatively impact their view of that retailer. Online Journey Hijacking is estimated to cost businesses between 2-5% in annual revenue.

Additionally, unsavory and inappropriate content also appears to web visitors, further damaging the business's brand equity.

Key Findings

- 2018 desktop infection rates were highest in the U.S. in the critical fourth quarter encompassing the peak holiday season shopping period, with 21.57% of all user sessions exposed to unauthorized ads. European desktop infection rates were highest in Q2 at 22.56%.
- The rate of infected mobile users significantly climbed in Europe during 2018 and peaked at 17.46% in Q3. In the U.S., 16.78% of mobile users were disrupted by Online Journey Hacking in Q4 2018.
- Users on all major desktop web browsers exhibited high infection rates. Apple Safari users were the most impacted for both desktop and mobile browsers with infection rates of 24.66% and 19.19% respectively.
- Desktop users in 2018 were most infected with injected ads when browsing online marketplaces (25.72%) and home retailer (23.13%) websites, while 21.63% of mobile users...when browsing footwear websites.
- Online marketplaces were most impacted by Online Journey Hijacking during Q4 2018 covering the holiday shopping season, with 32.94% of desktop sessions and 25.05% of mobile sessions disrupted by injected ads.
- 39.02% of all infected users were interrupted by banner ads when visiting a website, while 29.21% were disrupted by pop-ups. 28.05% encountered product ads and promotions.
- Visitors to subscription-based websites and online marketplaces were most exposed to invasive ads throughout 2018 with infection rates of 43.26% and 34.07% respectively.
- Infected users on both desktop and mobile converted at over double the rate of clean users after Online Journey Hijacking was blocked from interrupting their online experience.
- Checkout abandonment rates were dramatically lower for infected users that had unauthorized ad injections blocked from disrupting them at the last stage of their journey.

Online Journey Hijacking: How Many Users Are Impacted?

In order to assess the scale of Online Journey Hijacking, Namogoo's methodology uses the term infection rate, which refers to the percentage of user web sessions where one or more injections of unauthorized content are detected.

While the scale of infection varies between mobile and desktop devices and fluctuates among online product verticals and regions during different seasonal periods, Online Journey Hijacking impacts every business with a funnel that relies on attracting and converting web traffic.

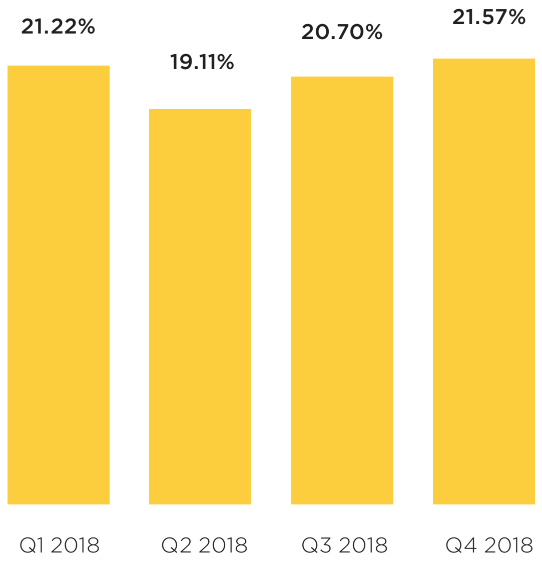
With more online brands today actively preventing Online Journey Hijacking, companies still vulnerable to this invisible client-side problem continue to have their substantial digital marketing investments into traffic acquisition and sales funnel optimization undermined as a result.

Desktop Infection Rates

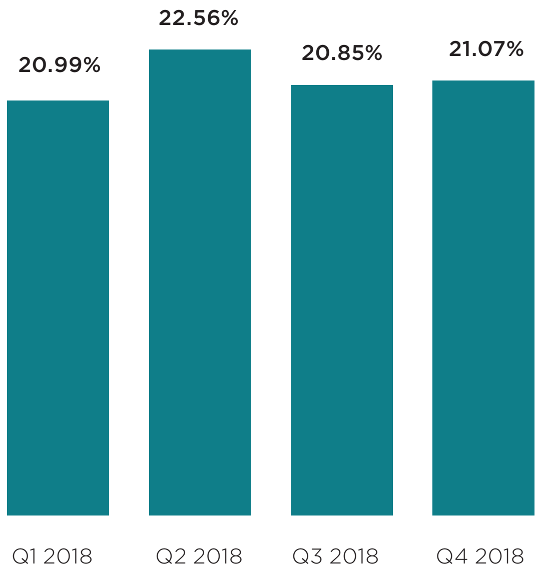
Infection rates for desktop users in both the U.S. and Europe substantially impact online revenue for businesses. Hovering at just over 20% of all website visitors, desktop users in both the U.S. and Europe infected with Online Journey Hijacking substantially impacted online revenue for businesses throughout 2018.

Infection rates were highest in the U.S. during Q4 2018, where 21.57% of all user sessions were exposed to unauthorized ads. In Europe, these disruptions peaked during Q2 at 22.56%.

Infection Rate in the US



Infection Rate in Europe



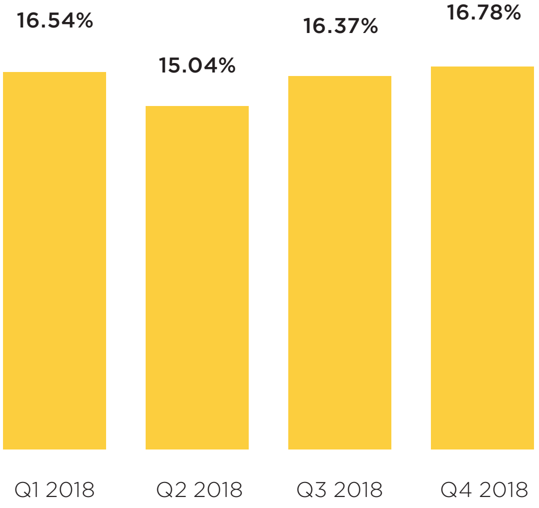
Mobile Infection Rates

Infection rates on mobile devices are generally lower than on desktops. This can be attributed to the fact that while mobile browsing is increasing, most conversions still occur on desktops. Since the business model of malware creators is based on affiliation commission, most of their activities target desktop-specific browser extensions and other web services.

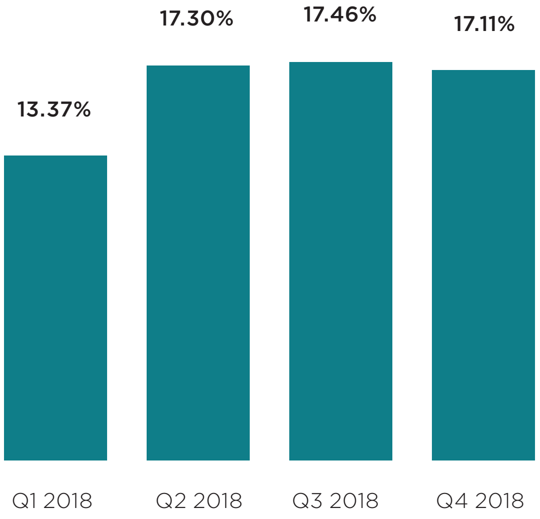
However, with mobile traffic continuing to grow, it's important to note that mobile users are less patient when it comes to disruptions, so the magnitude of these unauthorized distractions can be particularly harmful to online businesses.

Mobile infection rates in Europe rose markedly after Q1 2018, hovering at just over 17% of all site visitors.

Infection Rate in the US



Infection Rate in Europe



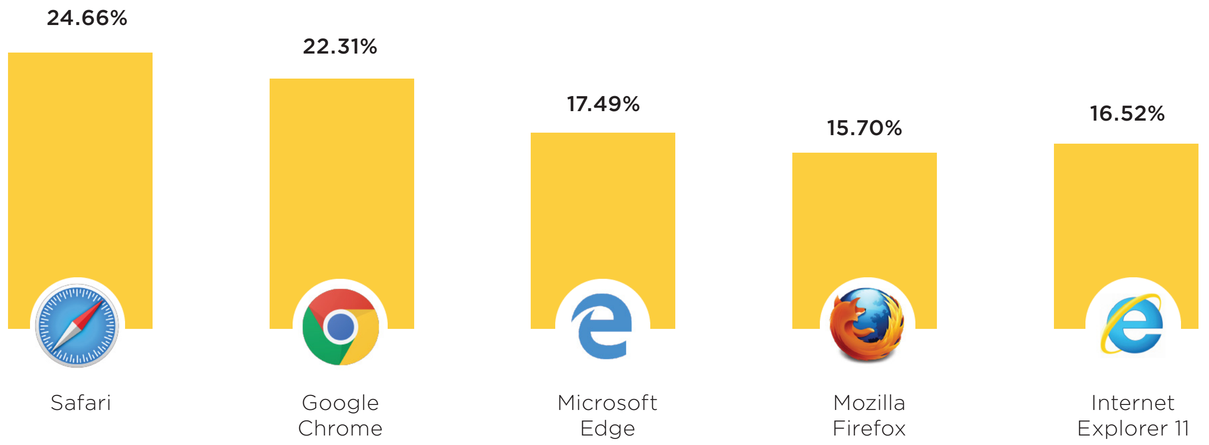
Online Journey Hijacking by Browser

No web browser is safe from Online Journey Hijacking. All of the web browsers most adopted by consumers have a significant percentage of infected sessions.

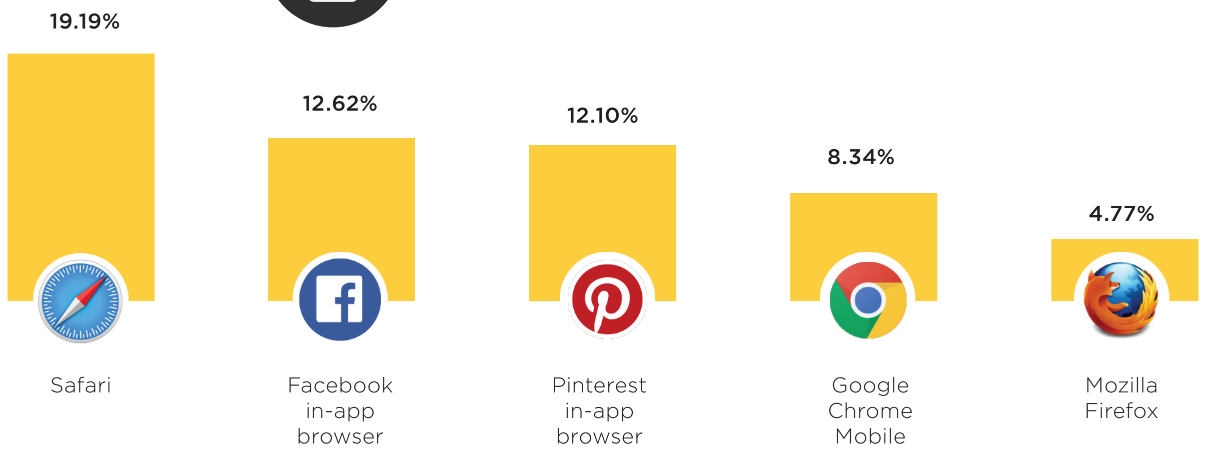
Perhaps surprisingly, Apple's Safari web browser had the highest infection rate for both desktop and mobile users at 24.66% and 19.19% respectively.

As in our previous report covering the first half of 2018, our data on mobile users revealed that Facebook's in-app browser had the second-highest infection rate. With more mobile users browsing content posted on Facebook, the vulnerability to unauthorized ad injections on the world's largest social media platform is a metric to watch going forward.

Infection Rates by Browser Desktop Users



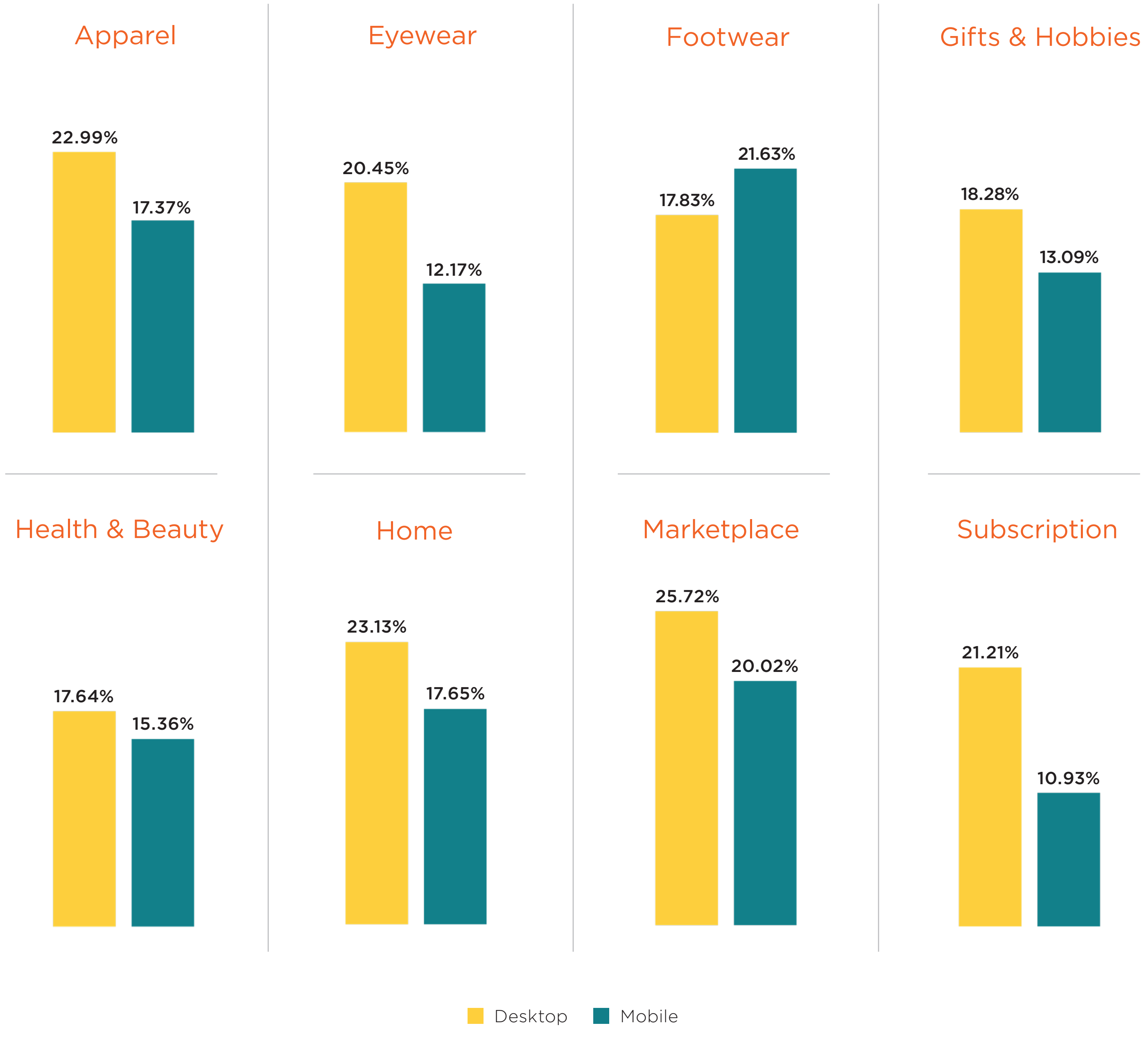
Infection Rates by Browser Mobile Users



Online Journey Hijacking by Vertical

Online Journey Hijacking impacts all verticals since it is caused by malware running on the consumer's device. Seasonal impact by vertical fluctuates, with some verticals more impacted than others depending on the time of year.

Infection Rates by Vertical



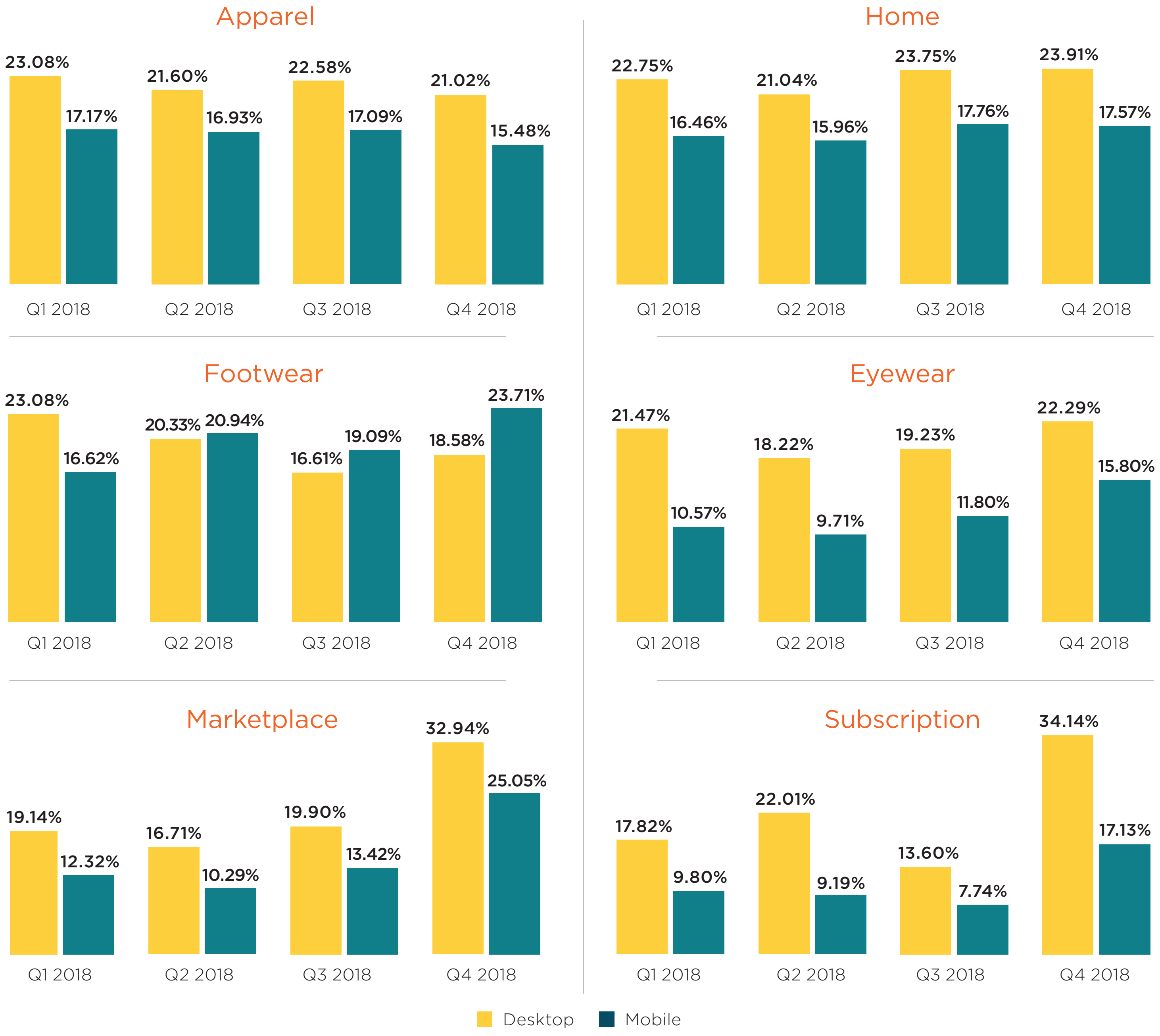
Infection Rates Increase Throughout 2018

Online Journey Hijacking rates increased during the critical fourth quarter, as ad injectors moved to capitalize on increased traffic and conversion during the peak holiday shopping season.

While infection rates rose in Q4 2018 for all major product verticals, we can see that subscription-based brands and online marketplaces experienced the most dramatic spikes. Infection rates more than doubled from Q3 to Q4 for desktop and mobile users (34.14% and 17.13% in Q4 respectively) visiting subscription-based websites.

Online marketplaces were also especially impacted during the 2018 holiday shopping season, with 32.94% of desktop visitors and 25.05% of mobile visitors disrupted by unauthorized ads.

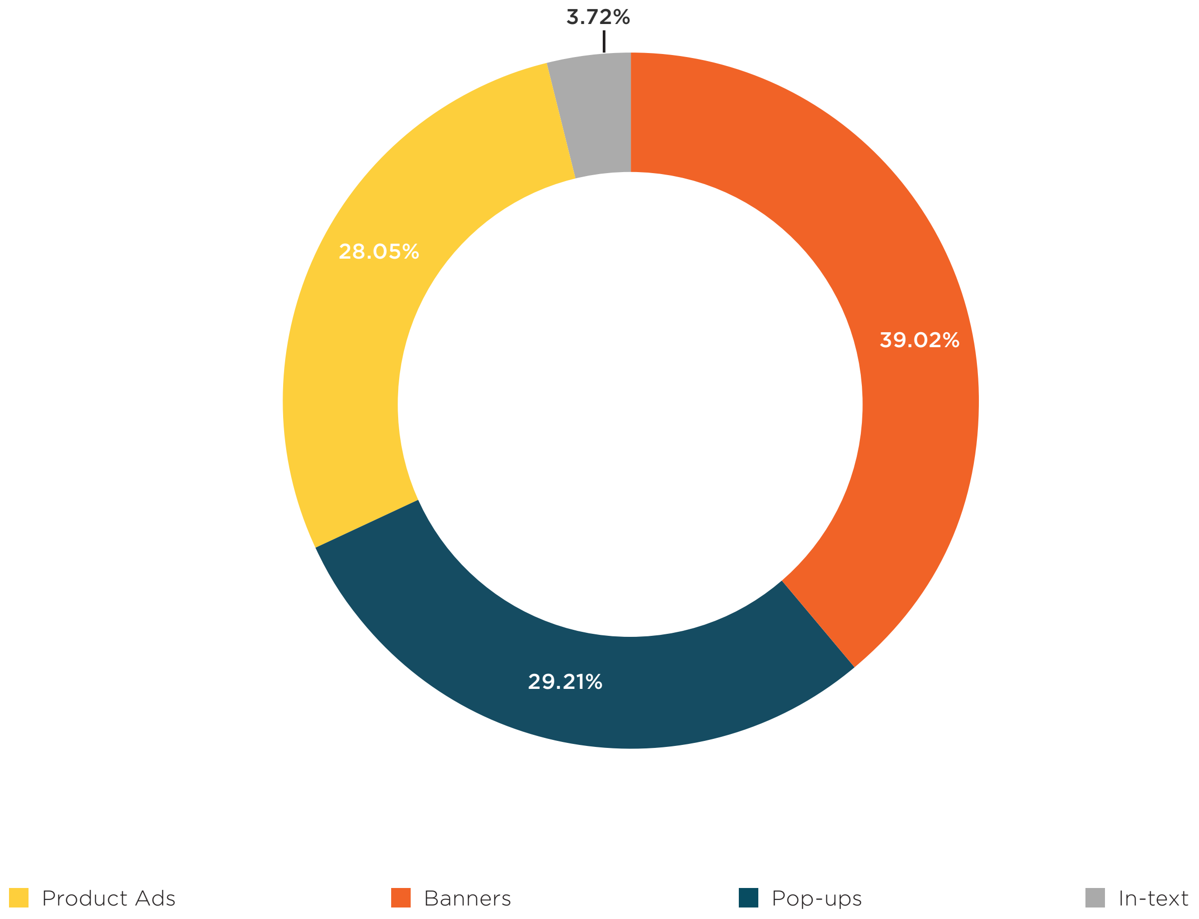
Infection Rates per Quarter by Vertical

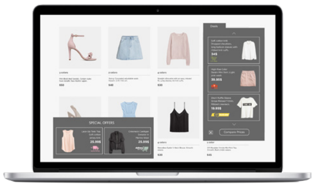


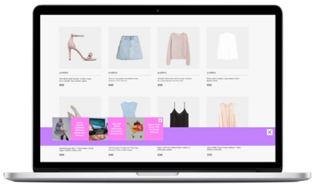
Online Journey Hijacking: Types of Injected Ads

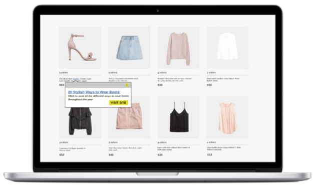
Online Journey Hijacking includes several types of unauthorized injected ads — each with its own method of targeting the user. Results of the analysis showed that 39.02% of infected users were interrupted by banner ads when visiting a website. This was followed by pop-ups, which featured in 29.21% of all infected sessions, followed by product ads, which featured in 28.05% of infected sessions

Ad Injections by Type







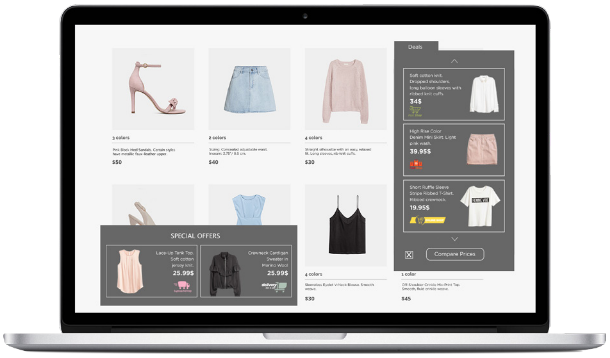


What Types of Ads Are Disrupting Users?

Namogoo defines these types of malware-driven injections as part of the consumer-side threat to online businesses known as Online Journey Hijacking:

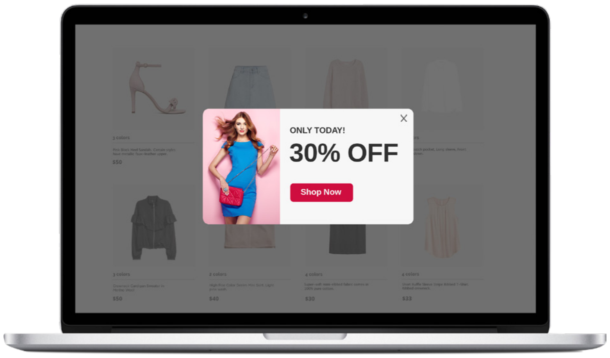
Product Ads

A product ad is a smart widget that displays to users specific products they're likely to be interested in based on their current or historic browsing patterns. With many sites regularly using related product recommendations, these types of ad injections can be very damaging; many are laid out subtly and appear as an integral part of the website.



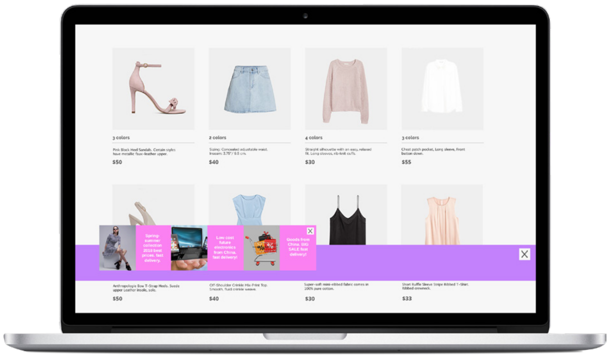
Pop-ups

Pop-ups can appear in front of a website and cover site pages and product displays with related products linking to other sites. They can also launch a new browser window on top of the one the user is viewing. Usually executed using some sort of JavaScript, pop-ups often divert the users' attention from their online journey.



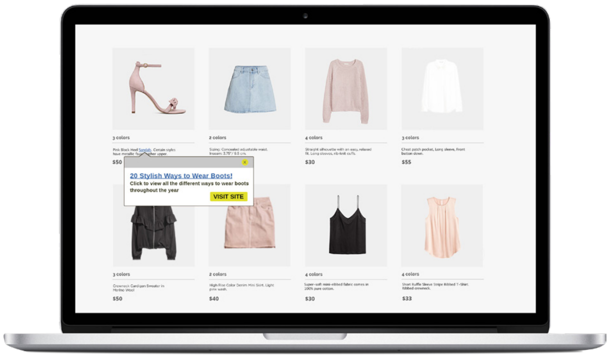
Banners

Also known as display ads, these are image-based advertisements that attempt to attract users' attention to specific brand offerings and other web services. The visual nature of banners promotes competing brands, adversely impacting the user's experience and perception of the hosting site's brand.



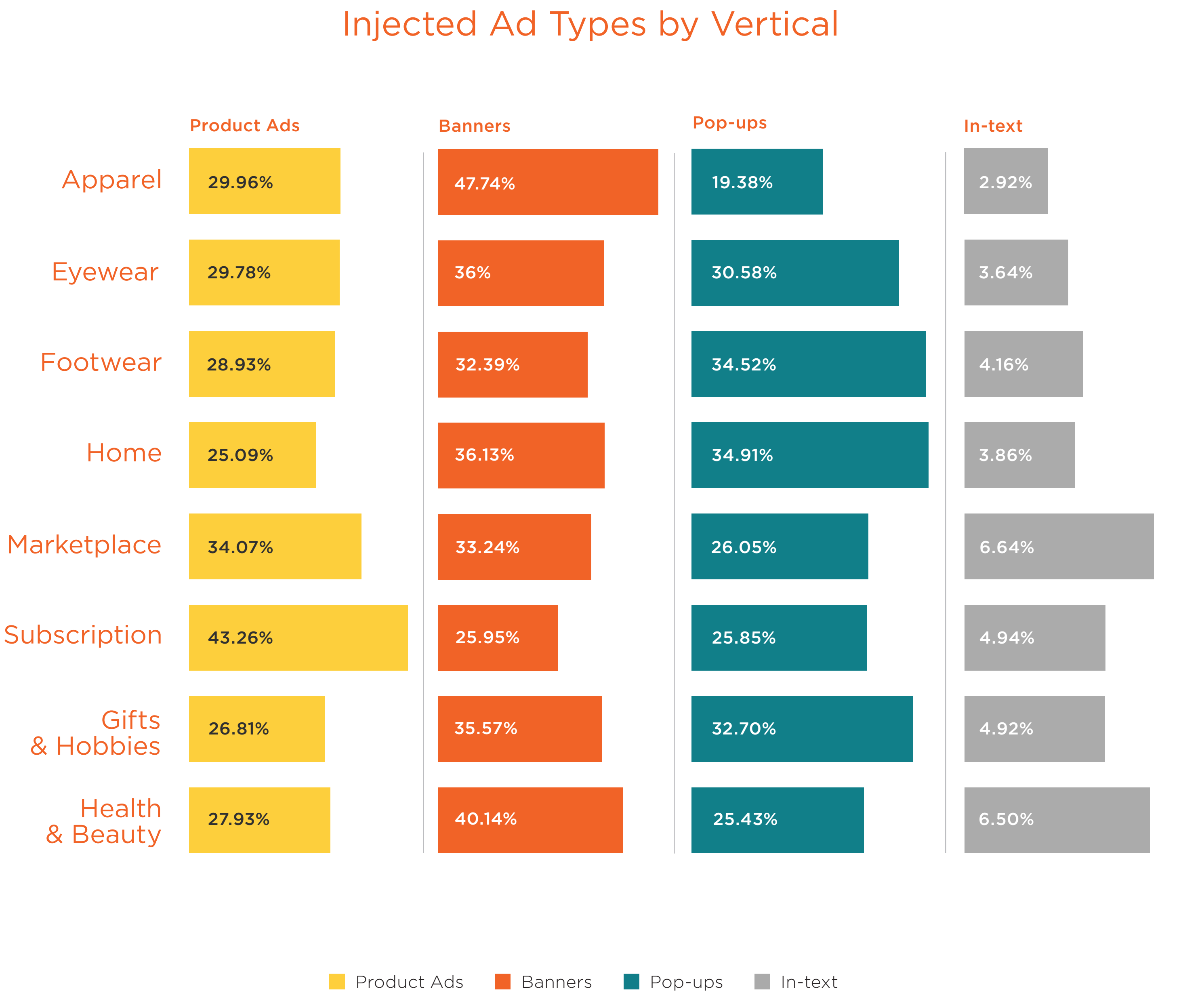
In-text redirects

In-text ads locate existing text links within website pages and redirect them to external links, and in many cases, competitor sites. These redirects are most often entirely invisible and can be especially disruptive to users trying to navigate through a site, search products, or click on register, sign-in or checkout links.


20 Stylish Ways to Wear Boots!
Click to view all the different ways to wear boots throughout the year
VISIT SITE

Types of Injected Ads by Vertical

We compared injected ad types by industry to learn which kinds of disruptions appear most prominently to infected visitors when browsing within different product verticals. Subscription-based websites were most targeted by related product ads, which appeared to 43.26% of all of their infected visitors. 47.74% of all infected users browsing for apparel products encountered banners in various sections of the site. Home and footwear brands were most impacted by pop-ups, which appeared to 34.91% and 34.52% of infected users.



2018 Conversion Rates by Quarter

One of the most common misconceptions regarding infected users is that they are less digitally savvy and are not as important a target audience for eCommerce businesses to focus on. For each quarter of 2018, we compared conversion rates for clean users against those of infected users after injected ads were blocked to provide them a distraction-free experience.

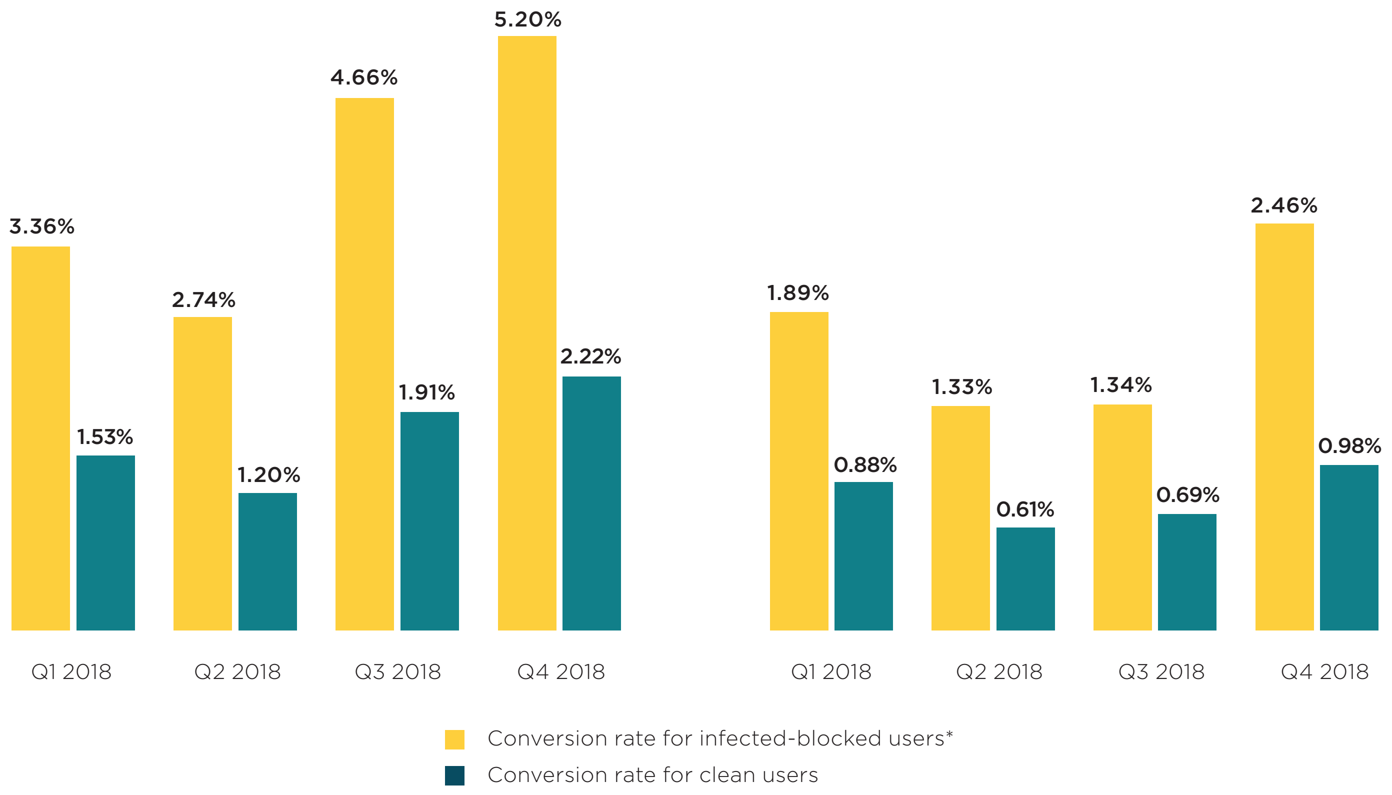
The charts below demonstrate the importance of the infected user segment to online business revenue. As seen below, previously infected users for whom injected ads were blocked from running converted more than twice as frequently as clean users. This was consistent across device types and regions examined.

While this may seem surprising at first, it actually highlights that the most active online shoppers are more inclined to download extensions and other web services that are bundled with digital malware — and consequently become infected. While unauthorized injected ads disrupt these users, they are still more active online consumers than the rest of the population. When these distractions are removed from their online experience, they end up converting at a much higher rate.

Protecting these high-converting users from disruptive injected ads becomes even more valuable for online businesses during busy shopping periods, as can be seen in the Q4 results below.

Conversion Rate: Desktop Users

Conversion Rate: Mobile Users



*Infected-blocked users are infected users for which injected ads have been blocked from running.

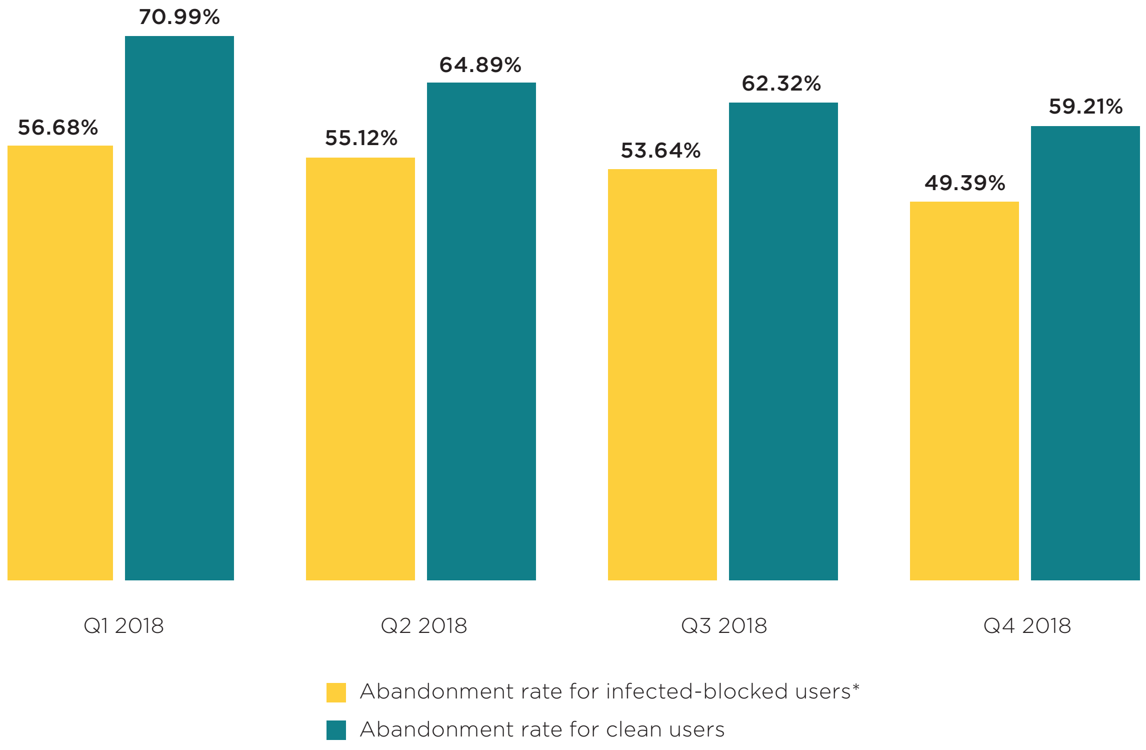
Checkout Abandonment Rates by Quarter

Similar to our conversion data, we compared checkout abandonment rates throughout 2018 for clean users against those of infected users after having Online Journey Hijacking removed from their experience. As can be seen below, checkout abandonment rates fell gradually for both of these segments each quarter and were at their lowest in Q4 2018. This is not surprising, considering that online purchases increase markedly leading up to and during the holiday season.

However, a wider gap can be seen when comparing infected users who had injected ads blocked and clean users that left at the checkout stage. Users previously infected with injected ads abandoned their carts far less frequently than clean users in every quarter, and during the critical Q4 2018 period, checkout abandonment rates for users previously impacted by Online Journey Hijacking were nearly 10% less than that of clean users.

As with our conversion findings, this highlights that the most active consumers are often exposed to unauthorized promotions as a result of downloading malicious content. Once these disruptions are removed from their experience at checkout, they abandon this critical stage of the sales funnel less frequently, and proceed to make their purchases.

Checkout Abandonment Rates: Infected vs. Clean Users



*Infected-blocked users are infected users for which injected ads have been blocked from running.

NAMOGOO

For more details, contact us at info@namogoo.com