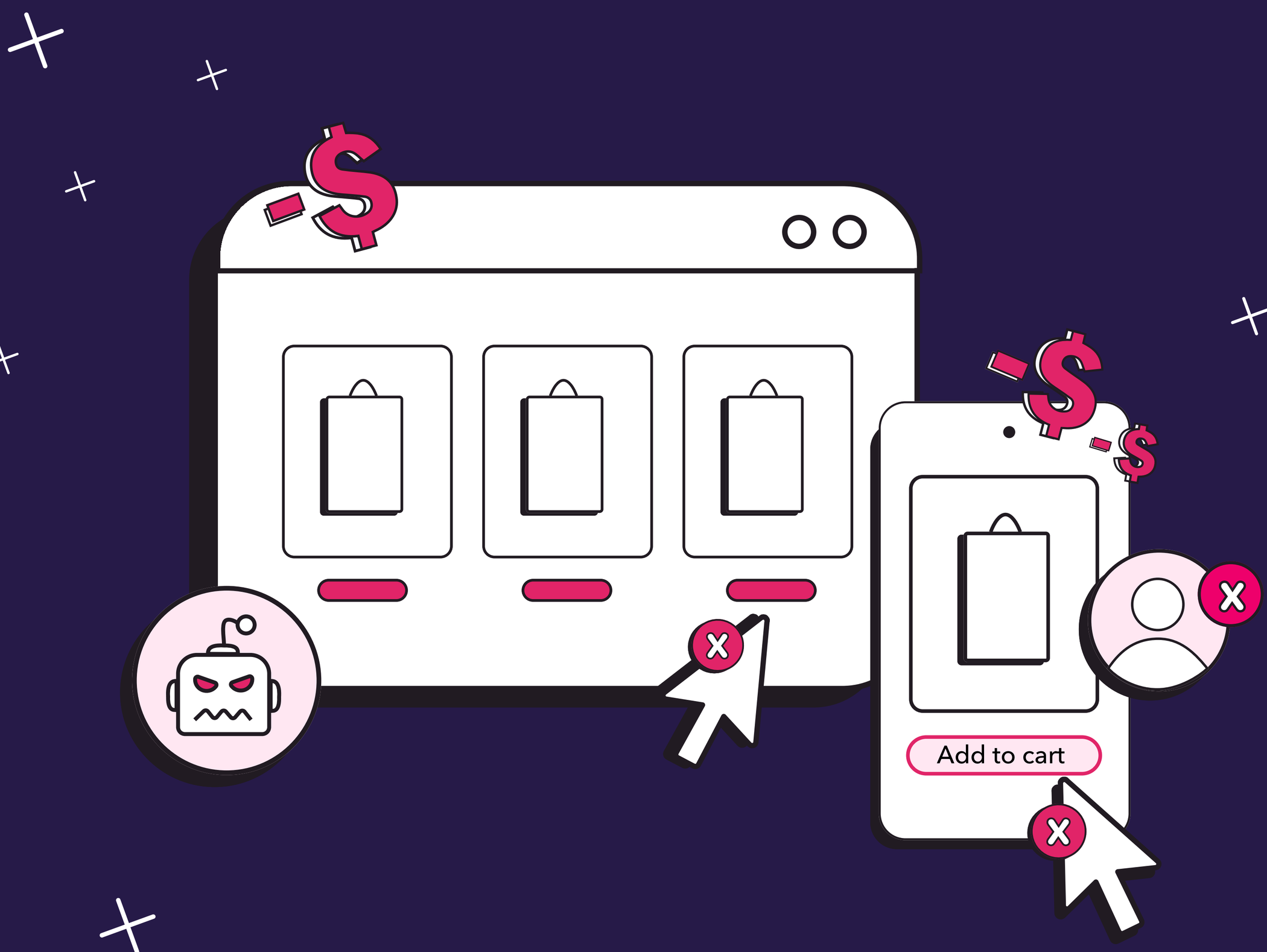
Fraud Season:

Black Friday & Cyber Monday Insights

Learn how bots & fake users impacted the 2023 holiday shopping season, and stay ahead of new threats this year



CHEQ

Introduction & Methodology

According to Digital Commerce 360, online sales continued to grow year over year during the 2023 holiday season. In fact, spending increased 4.9% since 2022 - indicating an industry trend. As online eCommerce continues to drive sales for retailers at an increasing rate, it becomes even more important that businesses make the most of every site visit, interaction, and transaction.

NRF National Retail Federation

"2023 Holiday to Reach Record Spending Levels"

CNN BUSINESS

"Energized shoppers break one-day holiday sales record"

AP

"American Consumers Are Feeling Much More Confident as Holiday Shopping Season Peaks"

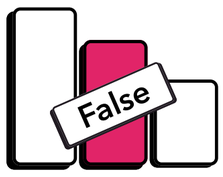
Unfortunately, bots and fake users can pose a significant threat to retailer goals.

In our recent comprehensive study, we analyzed **400 million website visits** to retail and eCommerce websites throughout the holiday shopping seasons of 2022 and 2023 (Black Friday through New Year's Eve), and applied more than 2000 cybersecurity challenges on each user including tests on behavior, device attributes, browser signals, and network indicators.

The threat types that were the most common across eCommerce websites were as follows:

- Malicious automation tools that can expose sensitive data and privileged customer information.
- User agent spoofing that can hide a user's true location and identity and bypass geographical exclusions.

Each of these threats can ultimately lead to:



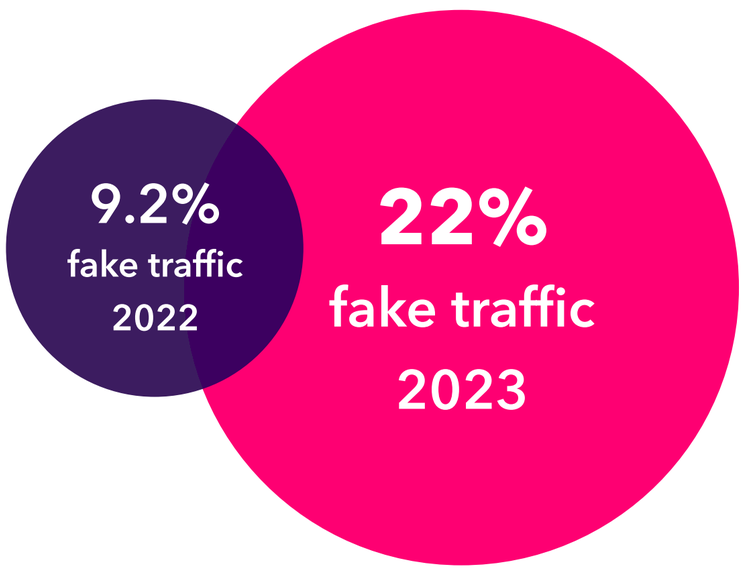
Skewed metrics that negatively influence decision-making.

Cart stuffing and denial of inventory that harms genuine customer experience.

Promotional and advertising abuse that disrupts marketing funnels and drains budgets.

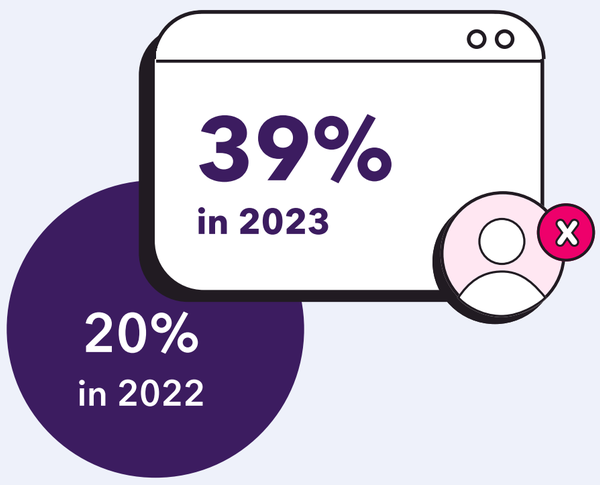
The Findings

Fake Traffic Rates During the Holiday Season

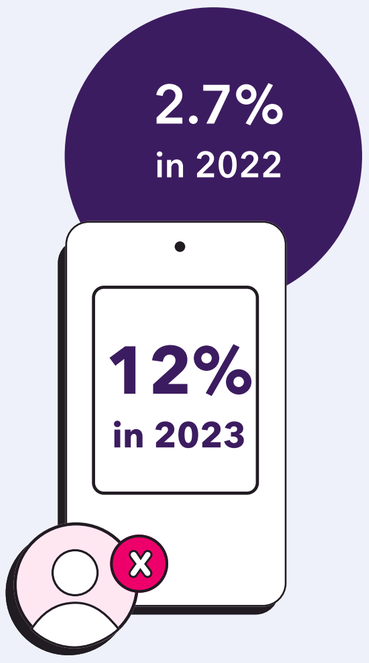


- 21.8% of traffic to retail websites during **Holiday Season 2023** (Nov. 24 - Dec. 31) was comprised of bots and fake users.
- 9.2% fake traffic during Holiday Season 2022 (Nov. 25 - Dec. 31)

Mobile vs. Desktop

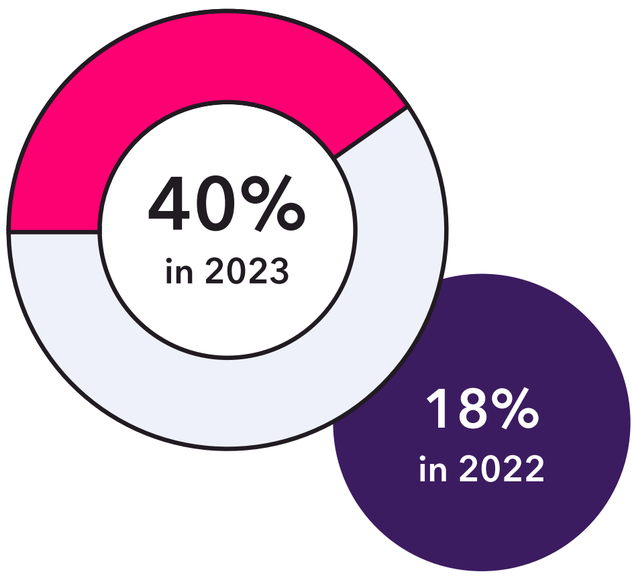


When looking at only Desktop devices in 2023, the fake traffic rate was even higher, at 39.2%. This could be due to the ease at which bots can be created and deployed via desktop.



For Mobile devices in 2023, the fake traffic rate was slightly lower than average, at 12.3%. However, this indicates that mobile fake traffic is still posing a significant threat.

As we studied the sources of fake traffic during the holiday season, one stood out above the rest: Direct Traffic. This type of traffic is commonly defined as users who type in a specific website URL as their destination, rather than clicking on a link within a search engine or arriving through other marketing tactics such as advertisements. An increase in authentic direct traffic can be a sign of strong brand recognition, but an increase in fake direct traffic could mean your business is falling victim to brute-force targeted attacks.



What eCommerce Leaders Can Do

Now that we have revealed the staggering information that about one in four visitors arriving on retailer websites during the peak of the holiday shopping season were bots or fake users, eCommerce professionals may be wondering what they can do to identify and mitigate potential threats in their day-to-day.

To address these pressing challenges, retailers are advised to take some proactive measures:

For unexplained spikes in traffic

If you're seeing spikes in traffic from sources or regions that you are not targeting, you should take a look at your analytics tools as well as any ad platforms or external tools that are driving this traffic and reset your geographical exclusions if necessary.

For low conversion rates

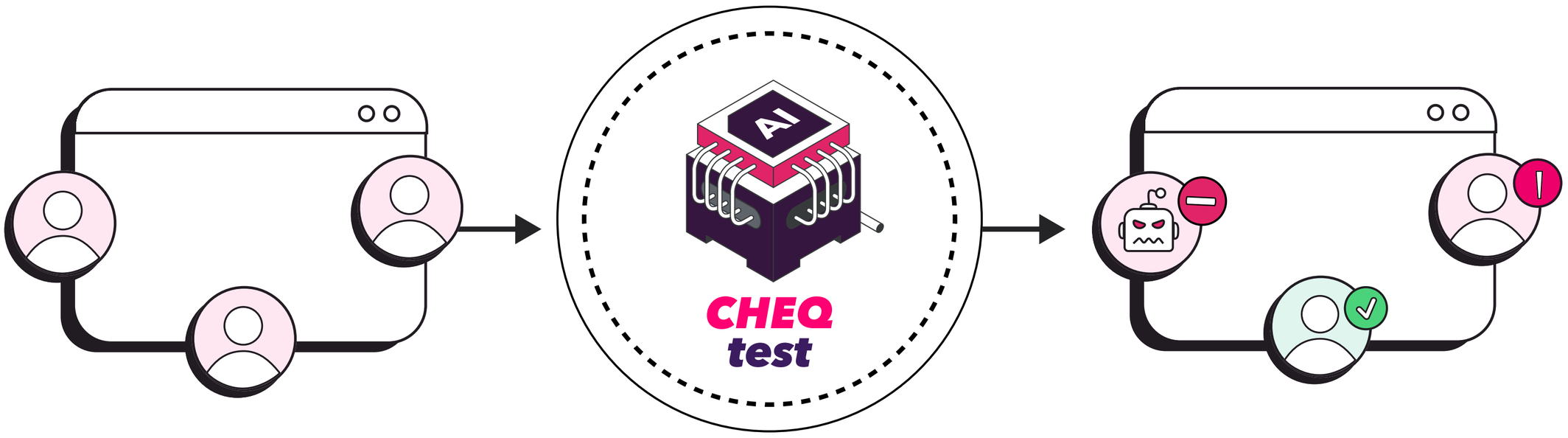
If you are noticing a lot of clicks and views of your promotional ads, but low conversions, you should dive deeper to determine the quality of user that is viewing and clicking on that ad. There is a possibility bots are infiltrating your campaigns and depleting budgets before real users can view them.

For increases in fake sign-ups

If you are concerned about your database or retargeting pools being polluted with junk leads, you should go through the exercise of cleaning up your database - removing legacy contacts, bounced emails, duplicates, and potentially emails from free services. You may also want to look for misaligned information such as company names that don't match the email domain, or contact names that don't match the email name.

For cart stuffing

If your customers are experiencing denial of inventory, and therefore you are experiencing a dip in sales, you should potentially reduce the amount of time an item is allowed to be sitting in a cart without completing a purchase in order to reduce bots from stealing this inventory away from paying customers.



The good news is that the team at CHEQ has years of experience tackling these specific issues and more.

Reach out today to learn more.

About CHEQ

CHEQ is the leader in Go-to-Market Security, trusted by over 15,000 customers worldwide to protect their metrics, marketing efforts, and customer data from those with potentially malicious intent online.

Powered by award-winning cybersecurity technology, CHEQ offers the broadest suite of solutions for securing the entire GTM org from threats to business continuity, brand reputation, and marketing effectiveness.

Schedule a live demo to learn how CHEQ can help you block fake traffic on your website and keep your go-to-market operation clear of bad leads and malicious actors.

Customers Love Us on G2