The 2023 Bad Bot Holiday Report

Grinch bots, carding, and account abuse during the holiday season

HUMAN

2023 Cybersecurity Holiday Readiness Report

Table of Contents

The holiday season is a huge target for cybercriminals. And it starts earlier than you think.

The holiday season is marked by family get-togethers and delicious food, but it's also become a huge target for cybercriminals. And it starts earlier than you think. While the rest of us are enjoying summer vacation, fraudsters are getting ready for the most wonderful time of the year. They spend the late summer and early fall:

- Harvesting sensitive data from breaches, leaky databases, phishing campaigns, and dark web lists
- Executing automated credential stuffing, carding, and brute force attacks to validate credentials, credit card numbers, and other PII
- Submitting fake leads and contaminating web engagement metrics

Cybercriminals use bad bots to prepare in the summer and fall, so they will be ready when the holiday season rolls around. These bad bots then launch large scale attacks during major online traffic periods and sales events. Holiday season bot attacks result in chargebacks and revenue losses, wasted marketing spend, and inaccurate data that skews business decisions for months to come.

Knowing exactly what attackers are up to is the first step to stopping them. The 2023 Bad Bot Holiday Report details attack patterns that HUMAN witnesses during the holidays and provides best practices to strengthen your defenses in preparation for the heightened bot activity.

*Fraudsters **set up their schemes in advance**, so they will be at the ready during holiday sales events.*

1.

Executive Summary

The 2023 Bad Bot Holiday Report details attack patterns that HUMAN has witnessed during the holiday shopping season.

Cybercriminals start attacking e-commerce sites before the human holiday rush begins

In the months leading up to Cyber Monday, **online retailers saw up to 199% more bad bot traffic** than the yearly average. Looking specifically at the period from September to November, bot traffic surpassed the three-month average starting October 1 and remained elevated for the remainder of 2022. Human traffic, on the other hand, did not consistently increase until late October and didn't reach its holiday peak until Cyber Week.

Bots wreak holiday havoc across the board

Due to increased attacks leading up to and during the holiday season, web applications experienced more bot attacks in the second half of last year as compared to the first. In the last six months of 2022, **carding attacks rose 161%**, **account takeover attacks rose 123%**, and **scraping rose 112%**. Overall, bot traffic accounted for 46.2% of total traffic in 2022, more than half of which was malicious.

Carding is a top threat to e-commerce retailers during the holiday season

In early November 2022, the percentage of **malicious checkout attempts out of total checkout attempts rose 350%**. The percentage of **carding attacks out of total checkouts increased 900%** in the days following Cyber Monday. This was likely due to bots continuing their attacks on e-commerce sites even after human traffic subsided.

2.

Methodology

The information in this report is based on a sample of the more than 1.5 trillion digital interactions across hundreds of applications, infrastructure elements, and endpoint devices in 2022, as verified by HUMAN. This is a subset of the 20 trillion online interactions that HUMAN observes each week. The data was pulled from the interactions we see and protect on behalf of our customers. Researchers used an out-of-band process, so there was no impact on the performance of monitored traffic or applications. The data was anonymized to preserve privacy, and any confidential company data was removed. Note that the data in this report has been normalized; the 25th percentile of outliers have been removed so as to not skew the results.

3.

Bot Traffic

In 2022, **bot traffic accounted for 46.2% of total traffic**. Bad bots are a security threat, executing account takeover, carding, scraping, and other automated attacks. But even good bots (like search engine crawlers) can negatively impact your business by contaminating your data. If almost 50% of the traffic you retarget with your marketing campaigns isn't human, **that's a lot of wasted marketing spend**.

Digital ad spending often increases during the holiday season, rising 13.7% in Q4 2022 than the previous quarter. CPMs and bid prices also increase. This means that the cost of targeting fake leads is even more significant during the holiday season, as is the negative impact of making campaign decisions based on contaminated data.

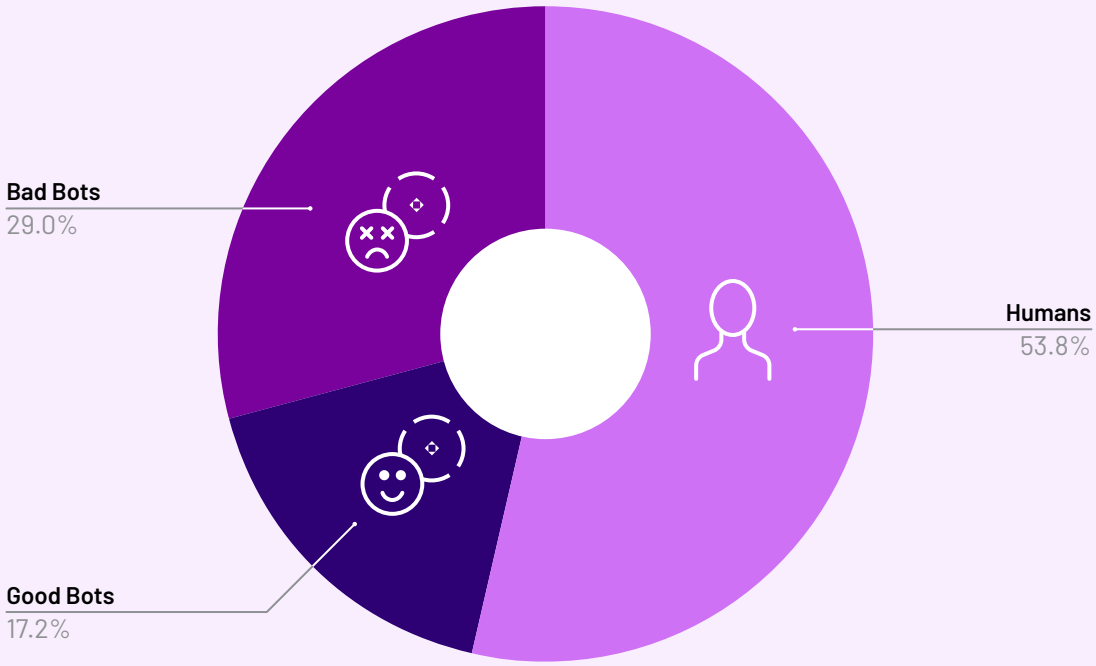

Figure 1: Traffic sources

4.

Peak Attack Days

Automated traffic is the highest during the holidays. Last year, bot attacks peaked in October and remained elevated through the rest of the holiday season. E-commerce brands saw **199% more bad bot traffic** on October 25 than the yearly average.

Looking specifically at the three month period from September to November, we can see differing traffic patterns for bots and humans leading up to and during the holiday shopping season. Human traffic rose steadily starting in early October 2022, but it did not reach above-average levels until late that month. The largest peak occurred during Cyber Week, when human traffic to e-commerce sites was **167% greater than the average** during those three months.

Bot traffic to e-commerce sites had already spiked several times by then. Holiday season bot traffic surpassed the three-month average in early October, reaching **131% on October 13** and **136% on October 25**. Even after those peaks, bot traffic to e-commerce sites remained **above 100%** of the average for the entirety of November.

Peak Attack Days

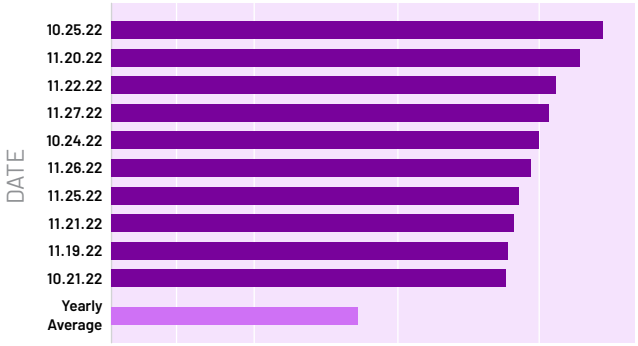

Figure 2: Malicious bot traffic during the 2022 holiday season

Web Traffic to E-commerce Sites During the Holiday Season

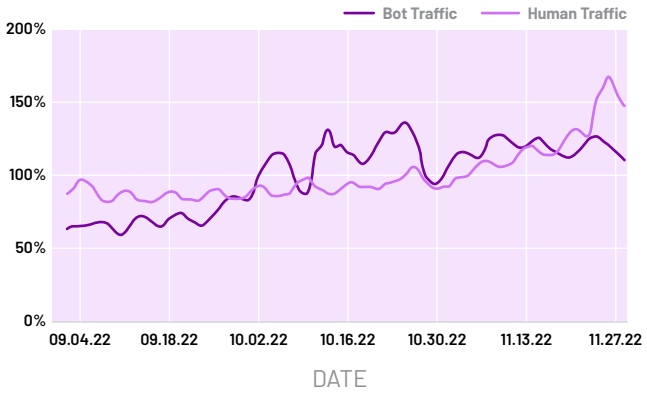

Figure 3: Traffic to e-commerce businesses during September-November 2022 as compared to three-month average

5.

Automated Attacks

HUMAN observed an increase in three common types of bot attacks throughout 2022: account takeover, carding, and scraping. Looking at the monthly percentages of these attacks, we see that all three follow a similar pattern. There is a spike in late summer, followed by another jump in late fall, and then above-average activity for the rest of the season.

Account Takeover

Fraudsters gain unauthorized access to online accounts via automated logins with stolen credentials. This allows them to make fraudulent purchases with stored payment data, drain account balances, steal gift cards and loyalty points, write fake reviews, submit fake warranty claims, and distribute spam and malware.

Carding

Attackers use bots to test stolen credit card and debit card data by making small purchases on e-commerce sites. Validated cards are used to make subsequent fraudulent purchases of products or gift cards, which are then converted into high-value goods and resold online.

Scraping

Bots crawl websites to capture pricing information, product descriptions, inventory data, and restricted content. Competitors use the information to gain a competitive advantage. Furthermore, if bad actors repost scraped content, it can damage the original site's SEO rank.

Account Takeover

For all industries, account takeover (ATO) attacks **rose 123% in the second half of 2022** as compared to the first half. This is due to spikes during the summer months and the holiday shopping season, when cybercriminals were validating stolen usernames/passwords in credential stuffing attacks and then using them to access compromised accounts. On average, **48% of total login attempts were malicious**.

For e-commerce companies specifically, account takeover accounted for **48.2% of all login attempts throughout 2022**. We can see a peak in August and again in October. ATO attacks remained elevated in November, but the percentage decreased due to a spike in legitimate traffic. Because holiday sales start earlier and earlier, cybercriminals, too, launch attacks earlier. This allows them to spread out their attacks, leading to a series of smaller attacks throughout the back half of the year, rather than a single large spike in November.

Account Takeover Attacks in 2022

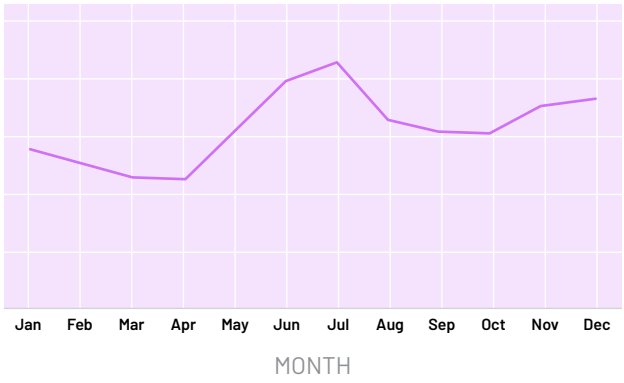

Figure 4: Amount of malicious login requests per month in 2022

Account Takeover Attacks on E-commerce

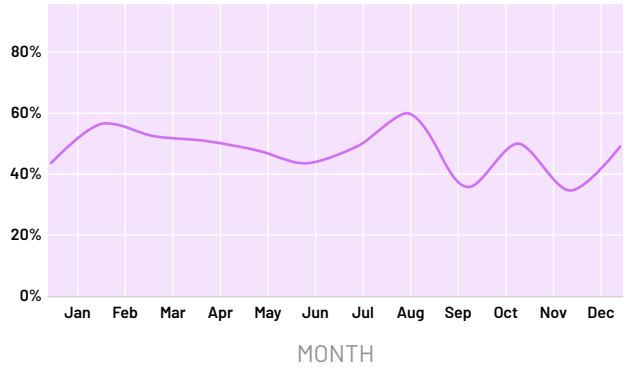

Figure 5: Percentage of malicious login attempts out of total login attempts on e-commerce sites in 2022

In 2022, there was a steady increase in malicious login attempts starting in September, with a sharp peak in mid-October. Malicious login attempts accounted for **more than 30% of login attempts**, up from 15% in September. Attackers were likely trying to get a large number of stolen accounts in advance of the holiday shopping season, so they could sell them on the dark web right before cyber week.

Account Takeover Attacks During the Holiday Shopping Season

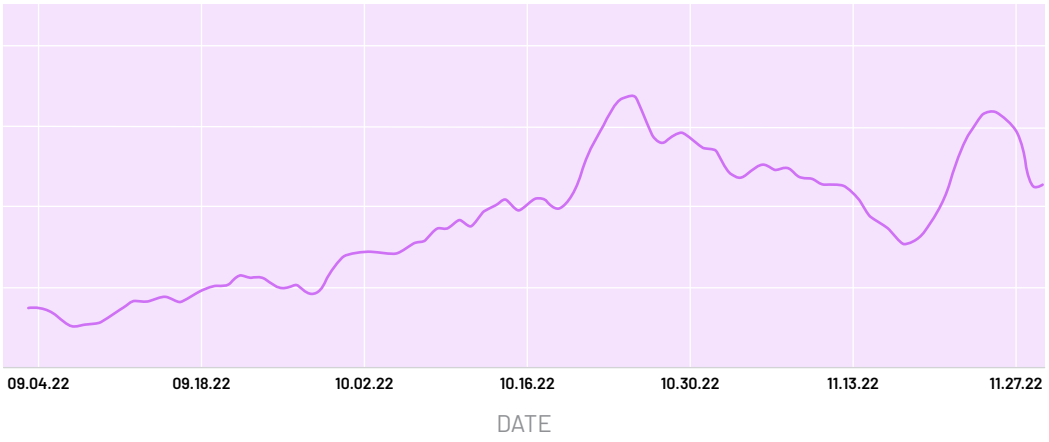

Figure 6: Malicious login attempts on e-commerce sites leading up to Black Friday 2022

Looking at malicious login attempts against total login attempts shows just how common these types of attacks are. **The percentage of malicious login attempts steadily increased as Black Friday approached**. The only sharp decrease occurred on Cyber Monday, likely because legitimate traffic surged that day.

Percent Account Takeover Attacks During the Holiday Shopping Season

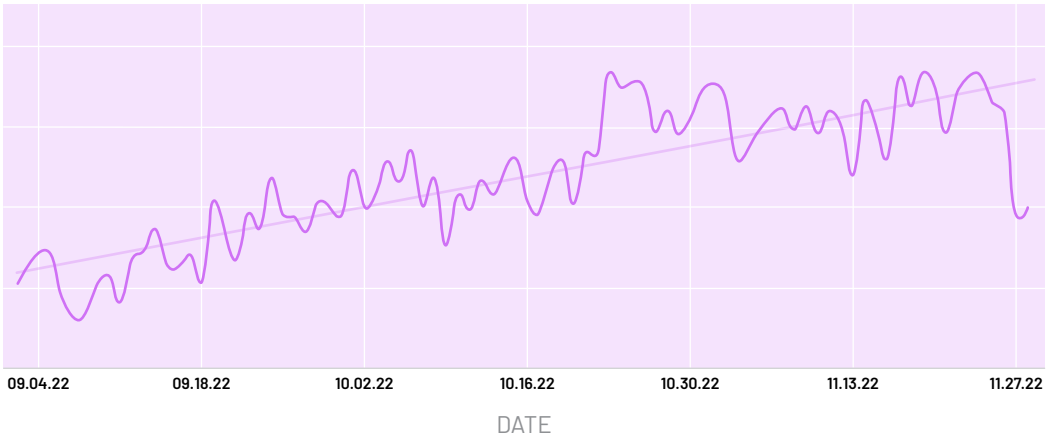

Figure 7: Percent malicious login attempts out of total login attempts on e-commerce sites during 2022 holiday season

Carding

The second half of 2022 saw a 161% increase in carding attacks during the second half of the year compared to the first half. Though carding attacks remained relatively stable throughout the year, there was a significant spike during the holiday shopping season.

For e-commerce alone, we see a large peak in the summer months, when **almost 30% of checkout attempts were malicious**. This was followed by another small peak in October and a jump during the holiday season.

Carding Attacks in 2022

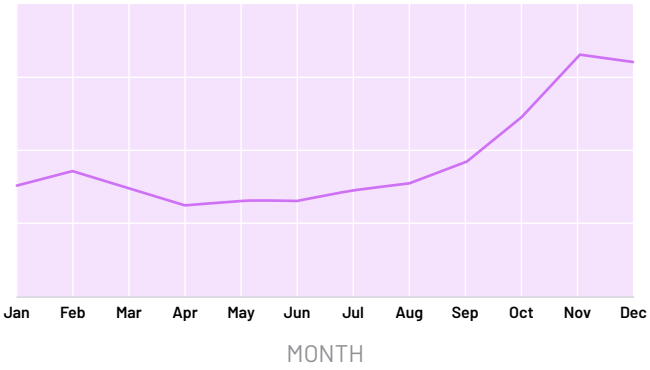

Figure 8: Amount of carding attacks per month in 2022

Carding Attacks on E-commerce

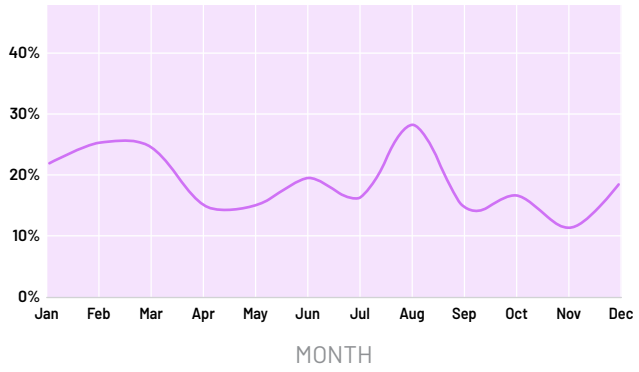

Figure 9: Percentage of malicious checkout attempts out of total checkout attempts on e-commerce sites in 2022

Now, let's zero in on the holiday shopping season. Carding attacks using both credit cards and gift cards had a few clear peak periods. The first wave occurred in early November, when the percentage of **malicious attacks out of total attacks rose 350%**. During this period, attackers made "dummy purchases," low-value transactions of random items, to determine if stolen credit card and gift card numbers were valid.

A second set of spikes happened during Cyber Week when cybercriminals attempted to validate stolen cards and make fraudulent purchases at the sales themselves. However, a similarly large increase in legitimate purchase requests meant that the percent of malicious carding attacks remained stable.

We also saw a **900% increase in carding attacks on the days following Cyber Monday**. This high attack volume is likely due to attackers continuing their efforts into the rest of the holiday shopping season, while legitimate traffic slowed after the Cyber Week spike.

Carding Attacks During the Holiday Shopping Season

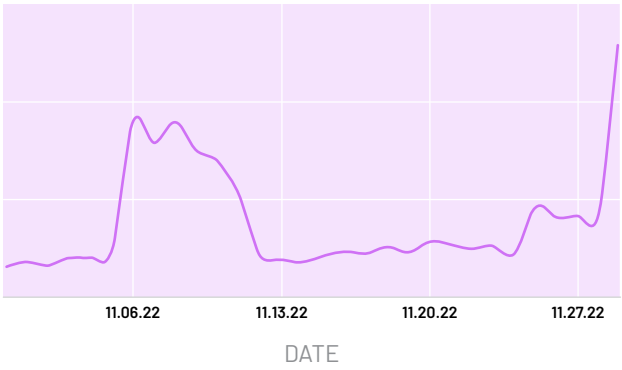

Figure 10: Malicious checkout attempts on e-commerce sites during 2022 holiday season

Scraping

Scraping attacks grew 112% in the second half of 2022 as compared to the first half. Though scraping isn't as closely tied to the holiday season as carding and ATO, increased activity during major sales events contributed to the overall increase in the back half of the year.

When we zero in on e-commerce businesses, we see that almost **40% of requests were malicious in August**, with another slightly smaller jump during the holiday season.

Scraping Attacks in 2022

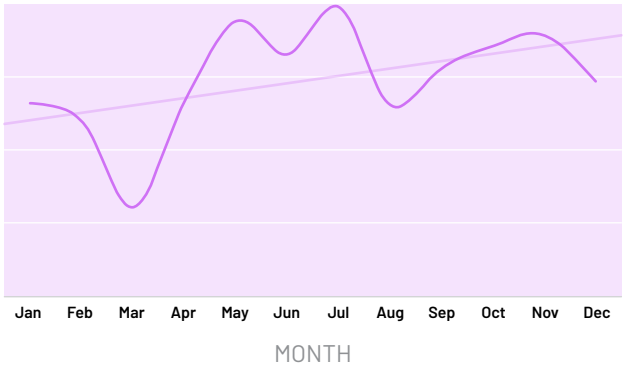

Figure 11: Amount of scraping attacks per month in 2022

Scraping Attacks on E-commerce

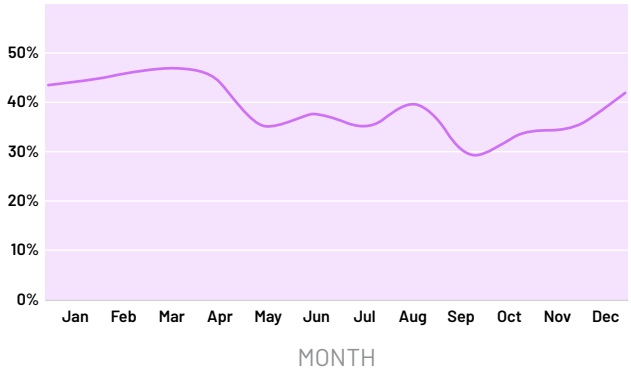

Figure 12: Percentage of malicious requests out of total requests on e-commerce sites in 2022

6.

Holiday Bot Insights

The holiday season is big business for cybercrime. That's nothing new.

→ But what is noteworthy is how attackers have shifted the timing of their operations. Instead of taking it easy over the summer and turning up the volume on a few well-known shopping days like Black Friday and Cyber Monday, fraudsters have started to take a wave-like approach. They prepare for their attacks at a time that may seem more insignificant, so they are in a stronger position to strike again during the holiday season.

Malicious bots are involved in 77% of all digital attacks, and they're in full force during the holiday shopping season. Stopping attacks as they come is critical and necessary, but it's a cat and mouse game. Only by flipping the economic script can organizations truly win against cybercriminals during the holiday shopping season and beyond. If it becomes more expensive for fraudsters to carry out their attacks than the potential payout, the cost-benefit analysis shifts. This is how HUMAN disrupts the economics of cybercrime.

*Malicious bots are involved in **77% of all digital attacks**, and they're in full force during the holiday shopping season.*

7.

Human Defense Platform

The **Human Defense Platform** offers advanced bot mitigation solutions to stop automated fraud on websites, mobile applications, and APIs. Using behavioral analysis and more than 300 machine learning algorithms, HUMAN detects and mitigates bad bots with unmatched speed, scale, and precision. HUMAN blocks bots at the edge, preserving page load performance and optimizing infrastructure costs. The solution uses a modern defense strategy to protect against account takeover, account fraud, transaction abuse, scraping, and data contamination.

Our unmatched **visibility** allows us to keep on the pulse of cyberthreats across the web, whether that's a bot attack on a single customer or a larger attack hitting multiple organizations. With our **network effect**, we share knowledge and deploy protections for all of our customers. We **disrupt** cybercrime with every mitigation action; we don't just block real-time threats, but execute a range of responses that increase the cost to bad actors and deter future attacks. By using modern defense to disrupt the economics of cybercrime, the Human Defense Platform delivers collective protection to combat tomorrow's cybersecurity threats, today.

*HUMAN uses a **modern defense strategy** to disrupt the economics of cybercrime. This approach is built on the pillars of **visibility**, **network effect**, and **disruptions and takedowns**.*

Modern defense is the fuel behind everything HUMAN does.

Visibility

Detection at unmatched scale

More than 20 trillion digital interactions are verified per week, and more than 3 billion devices are observed monthly to provide actionable intelligence.

Network Effect

Collective protection across the internet

2,500 dynamic network, device, and behavioral signals are parsed through 350 algorithms (technical, statistical, and machine learning).

Disruptions & Takedowns

Raise the cost of every digital attack

10+ years of experience combating adversary attack vectors, tools, and methodologies to disrupt cybercrime through takedowns, deception, and other innovations.

"When it comes to detection, nobody does it better than HUMAN. They make sure the bots get all the friction without touching the customer experience."

-**Security Engineer**, Global E-commerce Retailer

Contact HUMAN to see how we block bots and disrupt online fraud.

SOURCES: HUMAN: 2023 Enterprise Bot Fraud Benchmark Report; HUMAN: Holiday Bot Trends: Black Friday and Cyber Monday; Sensor Tower: Q4 2022 Pathmatics Data Digest

HUMAN

About Us

HUMAN is a cybersecurity company that protects organizations by disrupting digital fraud and abuse. We leverage modern defense to disrupt the economics of cybercrime by increasing the cost to cybercriminals while simultaneously reducing the cost of collective defense. Today we verify the humanity of more than 20 trillion digital interactions per week across advertising, marketing, e-commerce, government, education and enterprise security, putting us in a position to win against cybercriminals. Protect your digital business with HUMAN. To Know Who's Real, visit www.humansecurity.com.