HUMAN

MAXIMIZE YOUR CYBERSECURITY ROI

PROTECT YOUR ONLINE REVENUE SOURCE AS THE ECONOMY RISKS SLOWING DOWN

INTRODUCTION

Your Internet presence is the source of your online revenue. With the risk of difficult economic times ahead, protecting it from digital attacks is more important than ever. Many economies are showing more weakness than strength, with stock markets declining globally, inflation high and many organizations laying off staff. Protecting your most valuable assets — not least of which is your online business — will help you maintain profitability in the months and years ahead.

DIGITAL ATTACKS DURING A RECESSION

History has shown that criminal activity, and cybercriminal activity specifically, increases in times of recession. When the economy is tight, bad actors zero in on the places where money is flowing — and web applications and digital ad channels are high on the list. Not only are bad bots and other digital attacks a major security issue, they also have a large negative impact on brand reputation, operational costs, and marketing spend.

Here are some digital attacks that businesses should watch out for in today's climate:

Sophisticated Bot Attacks

Cybercriminals use sophisticated bots to conduct a range of attacks at scale. Modern bots are designed to mimic real human behavior, making them increasingly difficult to detect.

CARDING

In carding attacks, cybercriminals, (known as "carders") use bots to rapidly attempt small purchases using stolen credit card numbers on e-commerce sites. If the purchase goes through, the card is validated and can be sold at a higher price on the dark web. It can then be used to purchase electronics, gift cards or other high value items, which can then be resold for profit.

A carding attack not only affects the person whose card has been compromised. Payment networks such as Visa and Mastercard charge online merchants anywhere from $20-50 per chargeback, not to mention the cost of refunding customers. Payment processors can block all transactions if carding attacks are not handled quickly, which can result in lost retail revenue.

WEB SCRAPING

Web scraping is the process of using bots to extract content and data from a website. After scraping your content, competitors may repost it as their own, resell restricted content and data on the dark web, or otherwise use it to compete unfairly with your business.

Web scraping can increase your infrastructure costs, slow your site down or stop it operating completely, and lower conversion rates, losing all revenue until you have recovered. Research estimates that the annual business impact of web scraping is between 3.0% and 14.7% (median: 8.1% of annual website revenue) for businesses in the e-commerce, travel, and media industries.

HOARDING AND SCALPING

In hoarding attacks, bad actors use malicious hoarder bots to add an item thousands of times to a shopping cart over the course of a few days until the item's inventory is depleted. Scalping attacks take it a step further, purchasing sought after items — such as limited editions of sneakers, concert tickets, designer clothing, or hot toys — and reselling them at inflated prices on third-party sites.

Hoarding and scalping attacks keep high-demand items out of stock, tax your infrastructure, and reduce conversions and revenue. Customers become frustrated when bots snatch up inventory before they can purchase it, and they will turn to competitors to buy the products they seek.

SEE THE IMPACT

Leading Sporting Goods Retailer Prevents Carding Fraud

Cybercriminals use sophisticated bots to conduct a range of attacks at scale. Modern bots are designed to mimic real human behavior, making them increasingly difficult to detect.

A leading sporting goods retailer noticed an increase in carding attacks, specifically on its e-gift card balance checking page. They needed to block the bad bots, but couldn't risk mistakenly blocking human customers in the process. This required a solution that could detect the subtle behavioral differences between real human users and sophisticated carding bots, without generating false positives.

HUMAN was the clear solution, yielding the following results:

- During one high-volume attack, detected and blocked over 397K malicious requests while allowing over 383K legitimate requests to proceed without any impact to their experience'
- Cut the amount of time customers spent on verification pages nearly in half, from 66.09 seconds to 34.85 seconds
- Noticeable improvement in web performance because unwanted bot traffic was being blocked at the edge

By implementing HUMAN, the leading sporting goods retailer improved its security posture without negatively impacting customer experience. The company was able to stop carding fraud, prevent financial losses, improve website performance, and maintain customer satisfaction.

Account Fraud and Abuse

Both bots and human fraudsters can abuse accounts for profit. User accounts hold a lot of value—such as credit and debit card numbers, gift card balances, digital credits, loyalty points, and personally identifiable information (PII)—making them a rich target for cybercriminals.

ACCOUNT TAKEOVER

Account Takeover (ATO) is a form of identity theft in which cybercriminals gain unauthorized access to online personal or business accounts. Bots are often used to try to break into accounts at scale, using techniques such as credential stuffing, password spraying, or phishing.

Once the attacker gains access to the targeted account, they can transfer funds, use stored credit cards, deplete gift cards and loyalty points, redeem airline miles, submit fraudulent credit applications, plant ransomware or other malware, steal corporate data, and perform acts of cyberterrorism. Recovering lost accounts and remediating security issues costs your business time and money. ATO attacks increase customer support calls, harm consumer trust, and damage brand reputation.

ACCOUNT BALANCE THEFT

After taking over an account, fraudsters can drain the value stored therein. This includes account balances, loyalty points, and digital credits. These can be spent immediately or transferred to another account.

Account balance theft causes financial losses as merchants rush to refund customers. It increases calls to customer support, damages consumer trust in your business, and motivates buyers to shop elsewhere. Restoring a compromised account to its rightful owners consumes your team's valuable time and resources.

FAKE ACCOUNT CREATION

Fake account creation is the process of creating accounts using bogus or stolen identity information. Fraudsters can do this themselves or use bots to create fake accounts at scale.

Cybercriminals use fake accounts to exploit signup bonuses, post fake reviews, distribute malware, funnel money online, and inflate social media engagement. Fake accounts can also be used to execute phishing campaigns or access restricted content and data, which can then be scraped and resold.

SEE THE IMPACT

FanDuel Stops Account Fraud

FanDuel, a sports betting platform, was a large target for account takeover (ATO) attacks. The company was experiencing up to 10 million malicious login attempts per day. Given the high volume of malicious traffic and the sums of money held in customer accounts, FanDuel began searching for an automated solution that would protect its customers more effectively and not have an impact on performance.

FanDuel implemented HUMAN to solve its challenges and enjoyed these results:

- Blocked 99.9% of malicious inbound traffic to FanDuel's site, including requests that had already passed through a web application firewall (WAF)
- Reduced malicious login requests by more than 60% during a 24-hour period
- Provided an early-warning system for login attempts using stolen credentials to proactively mitigate account fraud

With HUMAN, FanDuel stops ATO attacks in real time and decreases the economic viability of credential stuffing attacks to deter future attempts. This helps preserve the company's reputation, maintain consumer trust, and protect revenue.

Client-side Attacks

Attackers can exploit vulnerabilities in client-side scripts to steal payment data and other PII. Malicious scripts load dynamically in users' browsers, so they can go undetected by typical web controls.

CLIENT-SIDE SUPPLY CHAIN ATTACKS

Up to 70% of code on websites consists of scripts from third parties and open source libraries. Because much of this code loads on the client side (in users' browsers rather than the central website server), it falls outside of the purview of typical web controls like a web application firewall (WAF). Static and external scanners may catch some anomalous code, but website owners lack complete visibility into the dynamic behavior of client-side scripts. This leaves a blind spot for attackers to exploit third-party client-side scripts.

Attackers may use known zero-day vulnerabilities in third-party JavaScript, take advantage of misconfigured permissions on Amazon S3 buckets and GitHub repositories, or induce insiders to give them access to website source code. Digital skimmers inject malicious code into the third-party scripts on your website to steal payment card data and other PII. These attacks are also called website supply chain attacks since the main threat comes from the third-, fourth- or fifty-party scripts and libraries used by websites.

PII HARVESTING AND FORMJACKING

PII harvesting (also called "formjacking") is a type of attack in which criminals collect names, addresses, and other PII from the forms on your website, typically on a login or checkout page. To execute formjacking, attackers exploit security vulnerabilities in client-side code to manipulate or inject malicious scripts that capture and exfiltrate PII from form submissions.

After collection, this data is used by the criminal or resold on the dark web for use in future cyberattacks. Suffering a client-side data breach can expose your business regulatory fines, lawsuits, and other financial losses. It can also lead to bad press and damage brand reputation.

DIGITAL SKIMMING AND MAGECART

Digital skimming and Magecart are types of formjacking attacks that target payment data specifically. Cybercriminals steal credit and debit card numbers from input fields on existing payment forms or hijack unsuspecting users to fake checkout pages. Malicious client-side scripts capture and exfiltrate the data, often without the user knowing.

Digital skimming and Magecart attacks can cause you to fall out of compliance with PCI DSS and subject you to regulatory fines. Other consequences include negative media coverage, loss of consumer trust, and remediation costs.

SEE THE IMPACT

Top 5 Global Airline Safeguards Against Client-side Data Breaches

This top 5 global airline lacked visibility into the behavior of client-side code, much of which was pulled from open source libraries and other third-parties. This made it difficult to catch and fix script vulnerabilities, which could be exploited in digital skimming and Magecart attacks. Following a Magecart attack on British Airways that resulted in a $20+ million regulatory fine, the airline wanted to ensure that it wouldn't meet a similar fate.

HUMAN offered the airline complete visibility and control over client-side scripts:

- Reduces risk of unauthorized data exposure and theft
- Protects brand reputation and consumer trust
- Helps avoid penalties and lawsuits by ensuring compliance with data privacy regulations, including GDPR, PCI DSS, CCPA, and CPRA
- Improves operational efficiencies by eliminating the manual analysis of website scripts

By providing continuous protection against client-side attacks, HUMAN prevents unauthorized exposure of the global airline's customer data.

Marketing and Ad Fraud

With their increasing spend and ever-evolving channels, digital advertising and paid marketing are appealing targets for cybercriminals.

PROGRAMMATIC AD FRAUD

Programmatically traded channels are particularly vulnerable to fraudsters who use bots to fake ad engagement.These advanced bots mimic human activity and imitate other devices using mouse movements, keystrokes, and fake browser behavior.

When fraudsters infiltrate the programmatic ecosystem, they steal more than just advertising dollars. Ad fraud damages the trust and the decisions the ecosystem delivers for digital advertising. The result is lower quality advertising inventory and decreased trust in the programmatic advertising system as a whole.

FAKE FORM FILLS

Fake form fills (or lead gen fraud) is where fraudsters drive bot traffic to landing pages. Sophisticated bots emulate human behavior and fill out forms with stolen or bogus information, stealing your marketing dollars.

Marketers require a steady flow of leads into their pipelines to meet key growth metrics. When bots are on the receiving end of marketing efforts, lead generation tactics do not deliver on results and budgets are wasted.

DATA CONTAMINATION

Bot traffic can account for up to 50% of your web traffic, skewing the data driving strategic decisions across your entire business. This can lead to erroneous conclusions about audience engagement, which may cause you to make bad business decisions about future investments, product and pricing plans, or campaign strategies.

Customers increasingly demand personalized experiences, which requires a deep understanding of your audience. Spammed comments and reviews, fake product interactions, and automated form fills may paint an inaccurate picture of user preferences and engagement.

MALVERTISING

Malvertising is when bad actors purchase and submit ads that appear to be normal, but execute malicious activity when displayed. This can include malicious redirects, client-side injections, unauthorized audio ads, clickjacking, video stuffing, and pixel stuffing.

Malvertising can have devastating effects, including revenue loss and billable hours for employees and specialists tasked with responding to attacks. In addition to these direct costs, businesses can face deterioration of user experience, lower customer satisfaction, and damage to brand reputation.

SEE THE IMPACT

AEG Presents Ensures Only Real Humans Receive Event Marketing

In an effort to eliminate marketing waste, AEG Presents sought to accurately detect the presence of sophisticated bots across its marketing channels and identify the sources supplying that invalid traffic. The company needed insights that could allow for subsequent marketing mix adjustments, improving performance and protecting against bot vulnerabilities.

AEG Presents deployed HUMAN to get the insights it was looking for:

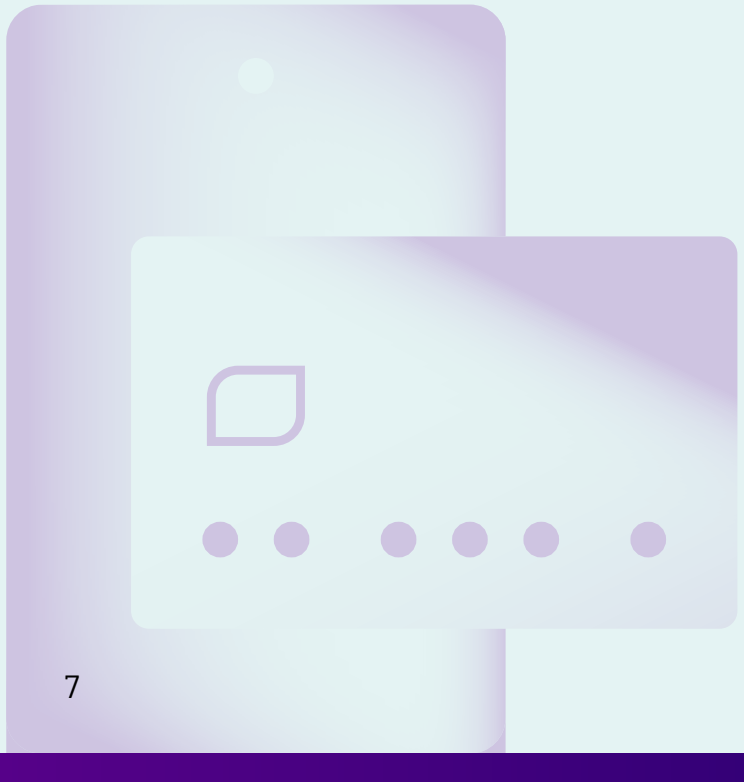
- Identified that 10.59% of total traffic represented invalid traffic from bots and other threats, and zeroed in on significant SIVT hot spots
- Found that more than 15% of traffic in one key tour effort came from bots, and identified particular display media channels as sources of SIVT
- Allowed AEG Presents to make real-time marketing optimizations, reducing bot traffic in future campaigns

Partnering with HUMAN allowed AEG Presents to reduce vulnerabilities within show marketing flows, specifically tied to on sale registrations in advance of the ticketing process.

THE ECONOMICS OF CYBERCRIME

Like any business task, cybercriminals have economic models that govern their attacks (albeit perhaps more informal than their business counterpart). Cybercriminals know that it will cost them $X to execute an attack and that they'll likely get $Y out of it — and in many cases, the economics are very much in their favor.

For example, a list of stolen credentials costs a few dollars on the dark web. Research estimates an 8% success rate (varies based on databases) if those credentials are used in a credential stuffing attack. Validated accounts can be sold for around $3 each. That's quite a profit. And there are similar gains across multiple types of digital attacks.



DISRUPT CYBERCRIMINALS' ROI WITH MODERN DEFENSE

In hard economic times, cybercriminals rush to execute the lowest cost, biggest benefit digital attacks. Protecting against these threats requires a layered defense model that not only stops attacks in real-time, but also proactively prevents future attacks. That is where a modern defense strategy comes into play.

HUMAN is powered by a modern defense strategy, which is built on the three pillars of global visibility, network effect and disruption:

Global Visibility

Detection at unmatched scale

More than 20 trillion digital interactions are verified per week, and over 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).

Disruption

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.

These core tenets allow HUMAN to not only protect customers against increasingly sophisticated digital attacks, but also to disrupt the economics of cybercrime. The Human Defense Platform works by raising the cost for cybercriminals to execute attacks and reducing the cost of collective defense. This is how HUMAN safeguards your online revenue source against evolving threats, in any economic climate.

ECONOMIC BENEFITS

By using a modern defense strategy, businesses can maximize their cybersecurity ROI with a number of tangible benefits.

Reduce Risk

Secure your online accounts from fraud and abuse with multi-layered defenses at each step of the attack chain.

Maintain Profitability

Avoid the costs of remediation and recovery, such as chargebacks, lawsuits, regulatory fines, and customer service and IT resources.

Preserve Brand Reputation and Consumer Trust

Instill confidence that your site is safe, without adding unnecessary friction to the user experience.

Improve Operational Efficiency

Free internal teams from spending time on manual security tasks and data cleanup. Maintain website performance and reduce infrastructure costs.

Optimize Marketing Spend

Ensure that only real humans receive marketing efforts. Stop losing marketing dollars to ad fraud, fake form fills, and signup abuse.

STRENGTHEN YOUR CYBERSECURITY POSTURE

With the risk of an economic slowdown ahead, now is the time to invest in a cybersecurity platform to combat digital attacks and online fraud. Protecting the source of your online revenue will have a positive impact on your bottom line, preserve your brand reputation, and increase operational efficiency. By implementing the Human Defense Platform, businesses can future-proof their protection and switch the economic odds in their favor.

Contact HUMAN to learn how we can strengthen your defenses against sophisticated bot attacks, account fraud and abuse, client-side threats, and marketing and ad fraud.

About HUMAN

HUMAN is a cybersecurity company that safeguards 1,200+ brands from digital attacks including bots, fraud and account 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.**