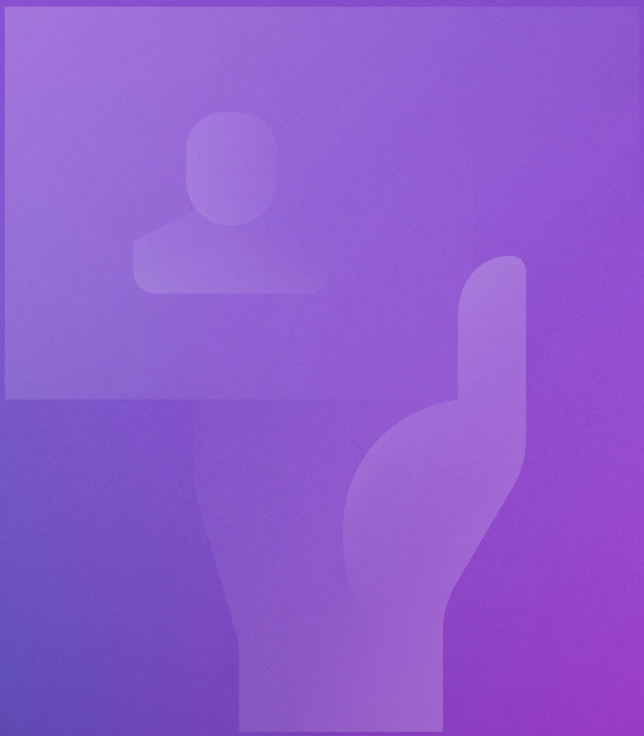
HUMAN

HOW TO STOP ACCOUNT TAKEOVER ATTACKS



PUBLISHER does not provide investment advice, is not a registered investment adviser or broker dealer and is not affiliated with a registered investment adviser or broker dealer. Nothing in this report should be construed as a recommendation to make, or not to make, any specific investments, or to buy, sell or hold securities.

INTRODUCTION

Account takeover (ATO) attacks can cost the average business up to 6.4% of their annual revenue generated from monthly active users. Cybercriminals commit many types of fraud after taking over an account, including making fraudulent purchases with stored payment methods, committing warranty fraud, submitting fake credit or loan applications, posting fake reviews and distributing spam or malware. ATO attacks damage brand reputation and consumer trust, put a strain on IT resources and result in significant financial losses.

ATO fraud attempts rose 307% from April 2020 to June 2021, averaging 82% of all login attempts in the second half of 2021.

HOW DO YOU SPOT AN ATO ATTACK?

The first and most critical step is knowing how to spot an ATO attack. Your security and revenue teams should watch for the following signs as potential indicators that an attack is either underway or has already succeeded in taking over your customers' accounts.

Hundreds or thousands of login attempts on accounts

This can indicate that a brute-force attack is taking or has taken place.

Spikes in helpdesk calls

Consumers will likely contact customer support if they are notified of an unauthorized login to their account or if they are locked out of their accounts due to an unauthorized password change.

Spikes in average purchase item price

Criminals often buy expensive items to make more money with fewer purchases to reduce the risk of being discovered.

Multiple, rapid fire changes to accounts

This is a big red flag. Users rarely need to change their payment info, address and password at the same time.

Inhuman user behaviors

Sophisticated ATO attacks use bots to navigate login pages or perform actions like purchasing merchandise. Bots scroll sites more quickly and precisely than humans do.

Unusually high numbers of chargeback requests

This can indicate someone is buying with an unauthorized account.

Odd IP behaviors

An increase in IPs associated with multiple devices, multiple accounts, or pointing into untraceable ranges — like you might see with a TOR client — can indicate that a fraudster is manipulating IPs to launch an automated ATO attack.

Spikes in password reset requests

After fraudsters take over an account, they immediately change the password.

Spikes in shipping address changes

This can indicate an ATO accompanied by shipping fraud, where criminals use drop shippers or mules to forward illegal purchases.

Spikes in reward points activities

Fraudsters either redeem bonuses for merchandise or services, drain them to sell on the dark web or add them to their own accounts.

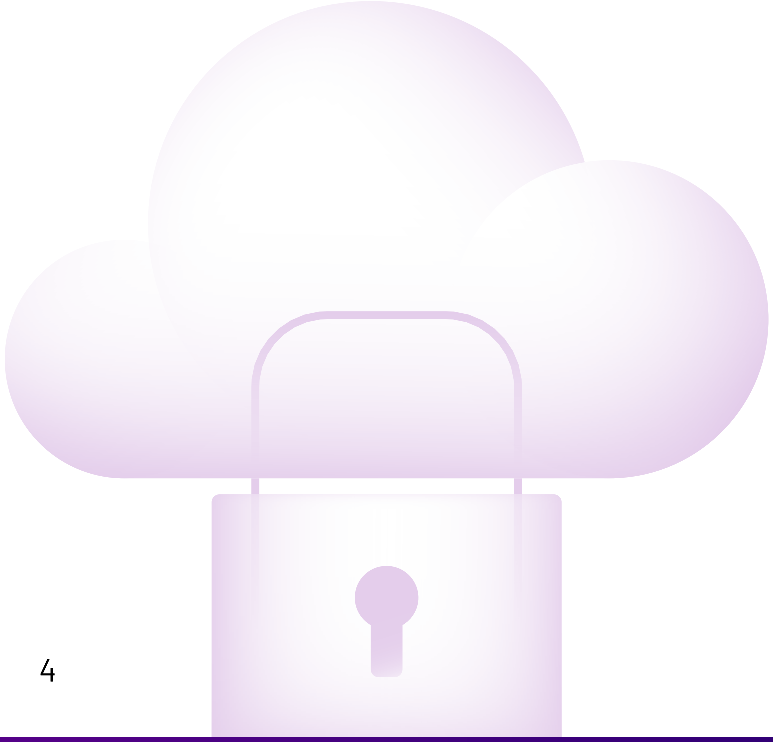
Slow application response time

Some ATO attacks unleash large numbers of requests that overwhelm your application and even your CDN.

These are all the basic warning signs. That said, more sophisticated attackers can better hide their actions by launching “low-and-slow” attacks. Such attacks are designed to spread more broadly across IP addresses and to limit attempts per second to a threshold to avoid tripping volumetric limits or trigger alerts.

Low-and-slow attacks often leverage botnets piggybacked on real browsers that are compromised by malware, but associated with legitimate IP addresses and human users. By the time they are noticed in log files, the attack has been going on for some time.

The 2022 Cyberthreat Defense Report found that credential stuffing and ATO were the #2 most concerning threat to web apps in 2022, up from #4 in 2021.



PROTECT YOUR USER'S ACCOUNTS WITH MODERN DEFENSE

ATO attacks are one of the fastest growing cyberthreats against businesses that collect, store and process customer information in online accounts. Successful attacks can cost millions of dollars, force unpleasant public disclosures, damage a brand, and upset customers and investors.

Protecting against ATO requires a layered defense model that not only stops attacks in real-time, but also proactively prevents future attacks. This is the core of the Human Defense Platform.

Powered by a modern defense strategy, the Human Defense Platform consists of three pillars:

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.

Taking a modern defense approach enables HUMAN to protect against account takeovers, raising the cost for attackers and reducing the cost of collective defense. Our solutions disrupt attack economics and stop cybercriminals at every turn.

For more information about how HUMAN stops ATO attacks, visit humansecurity.com.

HOW DO YOU STOP ATO ATTACKS?

The good news is that there are a number of steps that you can take to spot and block ATO attacks. Let's break them down into five steps.

1 Start with the Basics

Firewalls

Putting a web application firewall (WAF) in front of your application is table stakes. Firewalls enable you to block incoming traffic on specific ports and add signatures for specific types of attacks or exploits. Oftentimes, WAFs are included in application delivery controllers (ADCs). All major cloud providers offer WAFs and ADCs as a service.

Volumetric Traffic Detection and Analysis

Traffic and usage anomalies signal ATO attacks. Analyze hourly traffic patterns to login pages to identify usage spikes or anomalous patterns. If usage increases during what are normally off-hours, this could indicate an ATO attack. Likewise, abrupt changes in purchasing behavior, movement of loyalty points or mass password resets all are triggers that should kick off deeper forensics and stricter challenges for questionable activities and users.

2 Enable Additional Security At Login

Compromised Credential Monitoring

With real-time credential monitoring, businesses can detect and prevent users from logging in with compromised usernames and passwords. Acting upon the breached signal can stop a threat actor from accessing the account and warn real users that their credentials have been breached so they can take mitigating action.

Bot Management

Behavior-based, machine learning bot management solutions closely study all user behaviors to compare bot behaviors with those of legitimate users. These platforms spot small anomalies in user patterns—including on-page behavior, network signature and client and browser versions—in real time. Because machine-learning solutions grow smarter each day, they are able to identify even the most sophisticated attacks that might otherwise go undetected.

User Challenges

In some cases, additional security checks like CAPTCHAs and multi-factor authentication (MFA) can help weed out bad actors and malicious bots. However, these tools add friction to the user journey and drive abandonment. There are user-friendly alternatives that provide a better experience, but it is still crucial to only serve challenges to high-risk users and ensure that the false positive rate is low. Otherwise, you could be losing out on business.

3 Protect Accounts Post-Login

Continuous Risk Assessment

By continuously evaluating user activity post-login, businesses can safeguard accounts even if login checks fail. Taking note of the actions a user takes after logging in can surface anomalies that suggest fraudulent behavior, such as immediately changing the account password or disabling MFA. Account protection solutions can assess activity in real time and automatically intervene if the risk threshold is passed, stopping account abuse before the point of transaction.

Point-of-Transaction Protection

Identifying fraud at the point of transaction stops money from changing hands when a transaction is deemed invalid. This is a good last line of defense, but such solutions usually don't assess pre-transaction signals of account takeover and thus can't intervene proactively. If a bad actor even gets to the point of attempting card fraud, that means the account has already been compromised.

4 Deter Future Attacks

Proof-of-Work

Adopt technologies that make it more expensive for cybercriminals to complete their attacks on your site. One example of this is Proof-of-Work (PoW), a behind-the-scenes computational challenge that consumes a lot of energy and CPU cycles at scale. When bot operators encounter PoW, the cost-benefit analysis of the attack changes drastically. It negatively impacts their ROI and motivates them to choose a different target for future ATO attacks.

Password Resets

Resetting account passwords decreases the vulnerable attack surface by ensuring that accounts are no longer susceptible to future attacks. Forcing password resets adds friction to the user experience, and for many businesses this is not recommended. However, if you take a more strategic approach, it can make sense to force a password reset in certain situations, such as when credentials are known to be compromised or when post-login activities are suspicious.

5 Maintain a Feedback Loop

Threat Intelligence

Because ATO attacks are so dynamic with tactics and techniques that are constantly morphing, it is critical to have an active feed of threat intelligence information. This will help your team keep up with the latest research on attacks. Higher-end threat intelligence platforms have automated feeds or policy engines that tune firewall rules to block ATO attacks.

FANDUEL STOPS ACCOUNT TAKEOVER ATTACKS

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.

Sources:
Aberdeen Strategy & Research: Quantifying the Impact of Bad Bots on E-commerce Merchant Profitability
Aberdeen Strategy & Research: Quantifying the Impact of Credential Stuffing and Account Takeovers in Financial Services
CyberEdge Group: 2022 Cyberthreat Defense Report
PerimeterX: 2022 Automated Fraud Benchmark Report
Sift: Q3 2021 Digital Trust & Safety Index

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.**