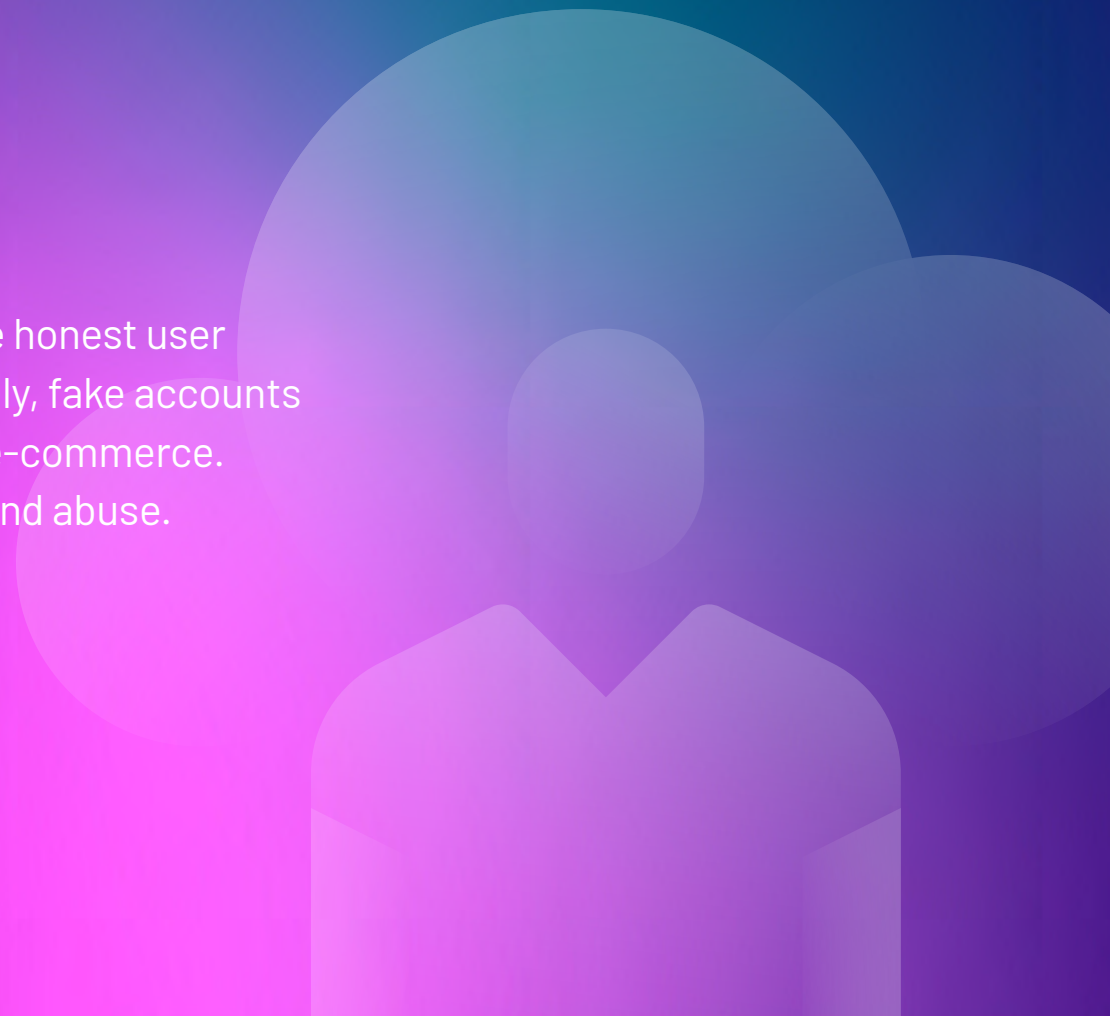




Taking Aim at Fake Reviews

Restoring Digital Trust

Consumers expect e-commerce sites to provide honest user reviews and secure transactions. But increasingly, fake accounts are compromising the integrity and security of e-commerce. Here's how technology combats account fraud and abuse.



Editor's Note

EDITOR'S NOTE

FAKE REVIEWS ARE A HOT TOPIC—AND HERE'S WHY

CRACKING DOWN ON FAKE REVIEWS

HOW HIGHER EDUCATION CAN COMBAT BAD BOTS, FAKE ACCOUNTS

SEVEN WAYS CYBERCRIMINALS COMMIT ACCOUNT FRAUD

GLOBAL E-COMMERCE RETAILER PREVENTS ACCOUNT TAKEOVER, CARDING ATTACKS, AND REVIEW FRAUD

HOW HUMAN CAN HELP

In the digital age, trust is increasingly difficult to establish and maintain—but also vital for e-commerce. Online consumers need to trust that businesses operate with integrity and transparency for them to transact online.

User reviews are part of forging this trust. According to 2023 Power Reviews, 98% of consumers believe that reviews are an [essential resource when making purchasing decisions](#), up from 89% in 2018.

But increasingly, consumers encounter fake or manipulated reviews on sites. This fake information distorts perceptions of products, services, and brands. Humans or automated bots may generate these reviews, and they erode trust between companies and their customers.

According to data, about half of consumers on a major e-commerce site have seen fake reviews, and 81% of [consumers have avoided a brand with fake reviews on its website](#). Moreover, fake reviews [cost billions every year](#).

In the following handbook on fake reviews and fake accounts, we explore how bot—or human-generated—fake information is having a deleterious impact on e-commerce.

In the first piece, "[Fake reviews are a hot topic—and here's why](#)," we explore how fake reviews are generated, and why governmental agencies are increasingly addressing them as a waste of consumers' time and money and a diversion from honest business practices.

In "[Cracking down on fake reviews](#)," we explore how the Federal Trade Commission, historically tasked with safeguarding consumers

from deceptive business practices, has trained its sights on fake reviews. It's a sign that the digital landscape—and user trust in that landscape—is central to a thriving e-commerce system.

In "[How higher education can combat bad bots, fake accounts](#)," we explore how malicious actors unleash bots on college campuses and create fake student accounts. But the harm doesn't stop there. Bots enroll in classes and deny real students seats, engage with faculty and staff, and post with fake accounts on discussion boards.

In "[Seven ways cybercriminals commit account fraud](#)," we enumerate ways that malicious actors commit fraud, such as creating fake accounts and creating fraudulent credit card applications with stolen information. We conclude with best practices to safeguard against fraudulent attacks.

Finally, in "[Global e-commerce retailer prevents account takeover, carding attacks, and review fraud](#)," a vitamin distributor suffered from volumes of malicious bot traffic that compromised customer information through account takeovers (ATOs), credential stuffing, and carding—and compromised the website's authority with bot-generated fake reviews. It successfully combated malicious bots with HUMAN. The result was a dramatic decrease in ATOs and in the company's ability to proactively prevent attacks.

Read on to learn more about fake reviews, fake accounts, and how HUMAN can help.

Fake Reviews Are a Hot Topic—and Here's Why

Companies and consumers increasingly recognize the negative impact of fake reviews. Now governmental agencies are addressing fake reviews to restore consumer trust.

Fake Reviews Are a Hot Topic—and Here's Why

EDITOR'S NOTE

FAKE REVIEWS ARE A HOT TOPIC—AND HERE'S WHY

CRACKING DOWN ON FAKE REVIEWS

HOW HIGHER EDUCATION CAN COMBAT BAD BOTS, FAKE ACCOUNTS

SEVEN WAYS CYBERCRIMINALS COMMIT ACCOUNT FRAUD

GLOBAL E-COMMERCE RETAILER PREVENTS ACCOUNT TAKEOVER, CARDING ATTACKS, AND REVIEW FRAUD

HOW HUMAN CAN HELP

If you operate in an industry where customer reviews and their influence are big business, you've probably noticed the buzz about fake reviews. Companies and consumers now recognize the negative impact of fake reviews, and governmental agencies are addressing fake reviews to restore consumer trust (read more on governmental response to fake reviews in "[Cracking down on fake reviews](#)").

Fake reviews influence consumers' views of a product, service, or brand. Humans or automated bots may generate these reviews, which are appearing with increasing prevalence on e-commerce sites. The net effect is to erode trust between companies and their customers.

In this article, we will cover recent developments surrounding fake online reviews, how common they are, techniques used to create fake reviews, and how HUMAN helps you combat them.

WHAT'S CHANGED?

Governmental agencies recently acknowledged fake reviews are a problem and are now taking action. The Federal Trade Commission (FTC) recently announced a final rule banning fake reviews and testimonials, stating, "Fake reviews not only waste people's time and money, but also pollute the marketplace and divert business away from honest competitors."

The U.K. government has also introduced a new law, part of which addresses fake reviews: "Under the rules, it will be easier for consumers to manage subscriptions by providing clearer pricing, banning fake reviews, and giving consumers greater control over what they are purchasing online."

For consumers and businesses alike, these are positive steps in the fight to combat online fake reviews.

"Fake reviews not only waste people's time and money, but also pollute the marketplace."

—The U.S. Federal Trade Commission

EDITOR'S NOTE

FAKE REVIEWS ARE A HOT TOPIC—AND HERE'S WHY

CRACKING DOWN ON
FAKE REVIEWS

HOW HIGHER EDUCATION
CAN COMBAT BAD BOTS,
FAKE ACCOUNTS

SEVEN WAYS
CYBERCRIMINALS COMMIT
ACCOUNT FRAUD

GLOBAL E-COMMERCE
RETAILER PREVENTS
ACCOUNT TAKEOVER,
CARDING ATTACKS, AND
REVIEW FRAUD

HOW HUMAN CAN HELP

HOW COMMON ARE FAKE REVIEWS?

Fake reviews are prevalent where opinion and influence matter. Online marketplaces where consumers compare reviews for goods, or travel and hospitality platforms where travelers want to choose their perfect destination are just a couple of common examples.

Positive fake reviews will make goods or services appear more attractive than they really are and negative fake reviews can be used to unfairly tarnish the reputation of competitors' offerings.

The scale of fake reviews is significant. Trustpilot noted in its 2023 [Transparency Report](#) that it removed 6% of reviews flagged as being fake; in 2024 Amazon [stated](#) that it had proactively removed more than 250 million suspected fake reviews; and Google [said](#) it had removed more than 170 million policy-violating reviews and more than 12 million fake business profiles on Google Maps in 2023.

In the U.K. [a government study](#) found that fake reviews are causing an estimated £50 million to £312 million in total yearly harm to U.K. consumers. HUMAN's own [Quadrillion Report](#) found that on average 218,000 fake accounts were identified and flagged per customer in 2023 (fake accounts are a common vehicle for the creation of fake reviews).

Compounding these stats are consumers themselves. A [study by Bazaarvoice](#) found that 75% of shoppers are concerned about fake reviews and 63% think that brands should be taking action on fake reviews.

HOW ARE FAKE REVIEWS CREATED?

There are two primary methods fraudsters use to post fake reviews. The first uses automation in order to drive scale. Typically, this method involves bots, which act as a force multiplier, posting large numbers

of fake reviews in a short period of time, far beyond the capabilities of a real person. Historically, these reviews would have been relatively easy to identify given poor grammar and spelling. Nowadays, fake review text can sometimes be indistinguishable from real reviews as fraudsters and their tools have become more sophisticated.

The second vehicle for fake reviews (often used in tandem with bots) is the creation of fake accounts, which in many cases is a necessary step to post a review. Again, this is typically performed on a large scale, with fraudsters creating large numbers of fake accounts in order to post fake reviews frequently. Legitimate accounts that have been compromised by an [account takeover](#) attack (ATO) are another common vector for fake reviews.

WHAT CAN ORGANIZATIONS DO?

Combating fake reviews requires solutions that excel at detecting sophisticated bots, the large-scale creation of fake accounts, and neutralizing account takeover attacks.

Advanced detection models that combine multiple techniques—including intelligent fingerprinting, behavioral analysis, mouse movement and browser analysis, predictive analysis, compromised credential intelligence and post-login analysis of account usage—are vital for your chosen solution.

The good news is that HUMAN covers them all.

We protect organizations around the world against automated fraud and abuse. See how HUMAN worked with a [leading global e-commerce retailer](#) to significantly reduce fake reviews and ATOs while improving operational efficiency.

Then learn how our [Application Protection](#) and [Account Protection](#) packages can help your organization to do the same.

Cracking Down On Fake Reviews: How the FTC's New Rule Targets Bot-Driven Deception

An FTC rule targets bad actors that use bots to generate fake reviews. Will it restore consumer trust in the digital landscape—and in user reviews?

Cracking Down On Fake Reviews: How the FTC's New Rule Targets Bot-Driven Deception

EDITOR'S NOTE

FAKE REVIEWS ARE A HOT TOPIC—AND HERE'S WHY

CRACKING DOWN ON FAKE REVIEWS

HOW HIGHER EDUCATION CAN COMBAT BAD BOTS, FAKE ACCOUNTS

SEVEN WAYS CYBERCRIMINALS COMMIT ACCOUNT FRAUD

GLOBAL E-COMMERCE RETAILER PREVENTS ACCOUNT TAKEOVER, CARDING ATTACKS, AND REVIEW FRAUD

HOW HUMAN CAN HELP

The FTC's latest [rule](#) isn't just another regulatory update—it's a direct strike against the people and organizations that are using bots to manipulate user reviews and sway public sentiment.

The Federal Trade Commission (FTC) isn't trying to outlaw bots entirely—it's the misuse of the tools for creating fake content that's in the crosshairs. And, it's about time. These bots aren't just misleading consumers—they're undermining the trust that's critical to both businesses and public agencies.

For businesses, this means protecting your bottom line. But for public agencies, the stakes are even higher. Fake reviews can twist public perception, lead to bad decisions, and erode the trust that's essential for keeping things running smoothly. Staying compliant? Yeah, it's not optional—it's necessary. Here's what you need to know to keep your reputation—and your integrity—intact.

THE EVOLUTION OF FAKE REVIEWS AND BOT INTERFERENCE

For years, the FTC has been on the front lines, safeguarding consumers from deceptive practices. But as the digital landscape evolves, so do the challenges the agency faces. Among the most pressing of these is the rise of fake reviews—now a rampant issue in online marketplaces. The people behind these misleading reviews are using bots to their advantage. These automated systems can churn out fake content on a massive scale, skewing perceptions and giving an unfair edge to those exploiting fake reviews for their gain.

On August 14, 2024, the FTC announced a final rule that bans fake reviews and testimonials outright. This new regulation doesn't just target the creation, sale, and purchase of fake reviews; it also gives the FTC the authority to levy civil penalties against those who knowingly participate in these deceptive practices. As Lina M. Khan, chair of the FTC, noted, this rule is a powerful step toward ensuring fairness and honesty in the marketplace.

UNMASKING THE BOT NETWORKS BEHIND FAKE REVIEWS

The problem isn't the bots themselves—it's how the bad actors are using them. These days, AI tools are driving the creation of fake reviews at scale, allowing bad actors to flood platforms with convincing reviews designed to boost their products, sway public opinion, or damage a competitor's reputation.

While bots themselves aren't banned, the FTC draws the line when bots churn out fake reviews. These bots—automated programs that mimic human behavior—can flood product pages with glowing endorsements for products they've never seen or bombard competitors with negative feedback. The new rule goes straight after these deceptive practices, recognizing the huge impact they have on consumer trust and market integrity.

Today's bots, powered by natural language processing (NLP), can generate content that's nearly indistinguishable from real reviews, making it harder to spot what's fake. That's why it's not just about banning bots—it's about cutting off the economic incentives that drive the misuse of these tools.

EDITOR'S NOTE

FAKE REVIEWS ARE A HOT TOPIC—AND HERE'S WHY

CRACKING DOWN ON FAKE REVIEWS

HOW HIGHER EDUCATION CAN COMBAT BAD BOTS, FAKE ACCOUNTS

SEVEN WAYS CYBERCRIMINALS COMMIT ACCOUNT FRAUD

GLOBAL E-COMMERCE RETAILER PREVENTS ACCOUNT TAKEOVER, CARDING ATTACKS, AND REVIEW FRAUD

HOW HUMAN CAN HELP

STEPS BUSINESSES NEED TO TAKE FOR COMPLIANCE


So, what do you need to comply with the new rule and protect your reputation—and platform—from the impact of bot-driven reviews? Here's how to protect your organization's integrity:

- **Deploy advanced bot detection systems.** Your first line of defense should be top-tier bot detection systems. Whether you're protecting a brand or a public agency's digital services, the HUMAN platform is designed to identify and block bots before they can create fake accounts and generate fake reviews, safeguarding site integrity from the start.
- **Develop a proactive review verification system.** Once fake accounts are blocked, your next priority is ensuring that humans are creating these incoming reviews and the sentiments are authentic. Set up a proactive system to verify the authenticity of reviews before they appear on your platform. Even with bot defenses in place, some fake accounts or reviews will always slip through the cracks, and this step helps catch those. Deploying a review verification system reduces operational overhead while ensuring users see only legitimate feedback.

- **Regularly monitor and audit reviews.** Sadly, you can't just "set it and forget it." Those pesky bots are always adapting. While manual monitoring might work for smaller platforms, the big players—like Amazon, IMDb, and others—need to rely on automated systems to continuously monitor reviews and user-generated content. Even the best bot mitigation systems need regular oversight to ensure they're working as intended. Automated tools can flag suspicious patterns, but consistent audits and adjustments are crucial to maintain the system's accuracy and adapt to evolving threats.
- **Remove accounts posting suspicious reviews.** Catching fake reviews is only half the battle—you've got to act on them too. When accounts are flagged for posting suspicious reviews, don't hesitate to shut them down. Automated tools can spot suspicious behavior, but it's up to you to keep your platform clean. Regularly reviewing and removing these bad actors will help preserve user trust.

EMBRACING A NEW ERA OF TRANSPARENCY

The FTC's new rule is a clear signal: the era of unchecked fake reviews is over. As bots continue to evolve, the stakes are higher than ever. Businesses and public agencies must not only comply with these new regulations but also proactively adapt to safeguard trust in this rapidly changing digital landscape.



How Higher Education Can Combat Bad Bots, Fake Accounts

Higher education has digitized dramatically, bringing clear benefits. But digitization has also allowed bots to steal financial aid and other resources from real students.

How Higher Education Can Combat Bad Bots, Fake Accounts

EDITOR'S NOTE

FAKE REVIEWS ARE A HOT TOPIC—AND HERE'S WHY

CRACKING DOWN ON FAKE REVIEWS

HOW HIGHER EDUCATION CAN COMBAT BAD BOTS, FAKE ACCOUNTS

SEVEN WAYS CYBERCRIMINALS COMMIT ACCOUNT FRAUD

GLOBAL E-COMMERCE RETAILER PREVENTS ACCOUNT TAKEOVER, CARDING ATTACKS, AND REVIEW FRAUD

HOW HUMAN CAN HELP

Since 2020, higher education has undergone massive shifts that have modernized the sector.

Over the past few years, propelled by the pandemic and increased availability of high-speed connectivity, the education sector has digitized at lightning speed. This shift has enabled remote learning, innovation, and streamlined administration.

Increasing digitization reflects where education is headed longer term. According to research firm Encoura, some 99% of university chief online officers [expect an increase in online instruction](#), up from [70% who expected one before 2020](#). Digitization has also enabled immersive hands-on learning experiences and [increases in research innovation](#). In administration, digitization has streamlined time-consuming tasks such as enrollment and ongoing student communications.

THE GROWING USE OF FAKE ACCOUNTS IN HIGHER EDUCATION

But the growing use of technology in education has also introduced new security threats. One is the use of [malicious bots](#), which are flooding higher-education systems. According to a CalMatters article, for applications at more than 100 California community colleges, [more than 20% of student "applicants" were in fact bots](#). These bad bots create fake accounts, enroll in classes, gain access to school services and, ultimately, steal money by applying for financial aid through these fake accounts. In many cases, these bots attack multiple universities simultaneously, which gives them reach and scale.

When bots successfully infiltrate university systems, they can wreak havoc, emailing students with seemingly legitimate ".edu" email addresses to perpetrate other attacks, skewing class enrollment numbers, and defrauding institutions of funds and resources. In some other cases, fake students post to class discussion boards and submit assignments, creating time-consuming work for professors to identify bots, and remove them from class rosters or remove their content.

HOW FAKE ACCOUNTS ARE AFFECTING HIGHER EDUCATION

With the return of in-person learning over the past couple of years, many school administrators hoped that the impact of malicious online traffic in campus life would subside. But, in fact, school administrators in the CalMatters article noted that the presence of bots has accelerated in 2024. Bots in education have had a variety of negative outcomes.

- Disrupting student learning, skewing data
- Stealing financial aid through fake accounts
- Wasting university resources
- Creating wasted costs in acquiring new students

Disrupting student learning, skewing data. As educational institutions digitize, many have turned to online systems. That shift has boosted bot enrollment in schools, particularly in online classes. As a result, bots can flood a course with enrollment requests. The deluge can block real students from getting seats in classes and also [skews data on true demand for that course](#). Because bots enroll in multiple institutions, it also skews data sector-wide.

Stealing financial aid. While financial aid scams aren't new, technology such as AI makes bot-driven fraud easier and more prevalent. According to the [HUMAN Enterprise Fraud Bot Report 2023](#), while legitimate traffic dipped in 2023, bad bot traffic rose by 102% year over year.

Further, [the Quadrillion Report: 2024 Cyberthreat Benchmarks](#), reveals that, in 2023 alone, more than 200,000 fake account creation attempts and 40,000 post-login account compromise attempts were identified per customer within many sectors. This scale of automated fraud highlights the increasing sophistication and volume of these attacks.

EDITOR'S NOTE

FAKE REVIEWS ARE A HOT TOPIC—AND HERE'S WHY

CRACKING DOWN ON FAKE REVIEWS

HOW HIGHER EDUCATION CAN COMBAT BAD BOTS, FAKE ACCOUNTS

SEVEN WAYS CYBERCRIMINALS COMMIT ACCOUNT FRAUD

GLOBAL E-COMMERCE RETAILER PREVENTS ACCOUNT TAKEOVER, CARDING ATTACKS, AND REVIEW FRAUD

HOW HUMAN CAN HELP

Wasting university resources. In addition to stealing money, “ghost students,” or bots, can use a school’s cloud storage, VPN, and other online services reserved for students, faculty and staff. They can also use newly acquired student email addresses to commit other scams.

Further, faculty at many colleges are spending valuable time trying to authenticate real students and reject fake bot students from registering for classes.

Increasing student acquisition costs. It also costs universities money to market to prospective students. Bots can drain marketing spend on targeting fake accounts rather than potential students. The acquisition cost for new students is high (\$2,795 per student for a four-year private college).

HOW HUMAN HELPS DETECT AND ELIMINATE MALICIOUS BOTS IN HIGHER EDUCATION

Maintaining a secure, fraud-free environment is essential for educational institutions. It’s vital not only to protect financial resources but also to ensure that real students can fully engage in their education without the disruptions caused by fake accounts and automated bots.

The [Human Defense Platform](#), including product suites [Application Protection](#) and [Account Protection](#), helps higher education combat these threats effectively. HUMAN technology safeguards institutions by blocking the automated creation of fake accounts and monitoring post-login activity for suspicious behavior, ensuring that your systems are secure and your resources are protected.

Key capabilities include the following:

Enhanced detection. HUMAN can prevent large-scale fake account creation at your institution, ensuring that enrollment data reflects genuine student interest and true class attendees.

Efficient response. By automatically detecting and responding to abusive behavior, HUMAN reduces the time your organization spends investigating threats, allowing the team to focus on true security concerns.

Cost reduction. HUMAN’s precise detection and blocking of fake accounts helps minimize financial losses associated with bot-driven fraud, protecting your institution’s financial aid funds and marketing investments.

Keeping your institution safe from fraud is not just about protecting money—it’s about ensuring that real students can learn, engage, and succeed in a secure environment.

[Learn more](#) about how HUMAN can stop bad bots, fake accounts, and fraud.

Seven Ways Cybercriminals Commit Account Fraud

Here are seven ways fraudsters can abuse compromised accounts—and tips to prevent bad actors from taking over customer accounts.

Seven Ways Cybercriminals Commit Account Fraud

EDITOR'S NOTE

FAKE REVIEWS ARE A HOT TOPIC—AND HERE'S WHY

CRACKING DOWN ON FAKE REVIEWS

HOW HIGHER EDUCATION CAN COMBAT BAD BOTS, FAKE ACCOUNTS

SEVEN WAYS CYBERCRIMINALS COMMIT ACCOUNT FRAUD

GLOBAL E-COMMERCE RETAILER PREVENTS ACCOUNT TAKEOVER, CARDING ATTACKS, AND REVIEW FRAUD

HOW HUMAN CAN HELP

No business wants to suffer an [account takeover](#) (ATO) attack, but few realize the true extent of the damage it can cause. Account takeover fraud resulted in nearly \$13 billion in losses in 2023, according to the [2024 AARP & Javelin Fraud Study](#).

Once a cybercriminal gains unauthorized access to a legitimate user account, the possibilities for fraud abound.

Here are seven ways that fraudsters can abuse compromised accounts, as well as tips to prevent bad actors from taking over accounts on your site.

1. Make fraudulent purchases

Consumers often store credit card numbers, gift card balances, loyalty points, and airline miles in their accounts for easier checkout. Attackers who gain access to user accounts are free to go on a shopping spree with the stored payment data, courtesy of the account takeover victim.

2. Commit warranty fraud

Fraudsters can look back in an account purchase history and then call customer support to complain that an ordered item was never delivered or arrived damaged and demand a replacement, shipped to their address. This can cost businesses inventory that they'll never get back.

3. Submit fake credit applications

Attackers can use the information stored in financial accounts, including names and Social Security numbers, to take out fake loans and lines of credit. They often quickly convert stolen assets into untraceable cryptocurrencies or move cash to jurisdictions where enforcement is light before fraud is suspected.

4. Create fake accounts

Cybercriminals can use the personally identifiable information (PII) stored in a compromised account to open fake accounts using that name across other sites. Fraudsters can use fake accounts to distribute malware, post fake reviews, and conduct other types of fraud.

Account takeover fraud resulted in nearly \$13 billion in losses in 2023, according to the 2024 AARP & Javelin Fraud Study.

EDITOR'S NOTE

FAKE REVIEWS ARE A HOT TOPIC—AND HERE'S WHY

CRACKING DOWN ON FAKE REVIEWS

HOW HIGHER EDUCATION CAN COMBAT BAD BOTS, FAKE ACCOUNTS

SEVEN WAYS CYBERCRIMINALS COMMIT ACCOUNT FRAUD

GLOBAL E-COMMERCE RETAILER PREVENTS ACCOUNT TAKEOVER, CARDING ATTACKS, AND REVIEW FRAUD

HOW HUMAN CAN HELP

5. Funnel digital currency on marketplaces

Fraudsters may create fake accounts on the marketplace to offer fake products or services. Next, they take over legitimate accounts and use stored funds to purchase their own fake services. This allows them to secure the digital currency immediately and then cash it out little by little so the fraud goes unnoticed.

6. Post fake reviews

Fraudsters can post fake reviews using compromised accounts, artificially disparaging or praising a product or service. This is a way for cybercriminals to damage a competitor's reputation or promote their own product or service.

7. Distribute malware

Fraudsters commonly distribute malware through infected links in phishing emails or spam messages on social media. When a bad actor takes over a legitimate account, they can send a malicious link to that person's address book and trick recipients into believing it was sent from a trusted friend.

Because it is used to steal login credentials, payment data, and other PII, malware paves the way for additional account takeover attacks and begins the attack lifecycle all over again.

DON'T LET CYBERCRIMINALS TAKE OVER YOUR USERS' ACCOUNTS

Account takeover can have long-lasting repercussions for online businesses, including significant financial losses, damage to brand reputation and consumer trust, and operational inefficiencies.

So, how can brands protect themselves and their customers?

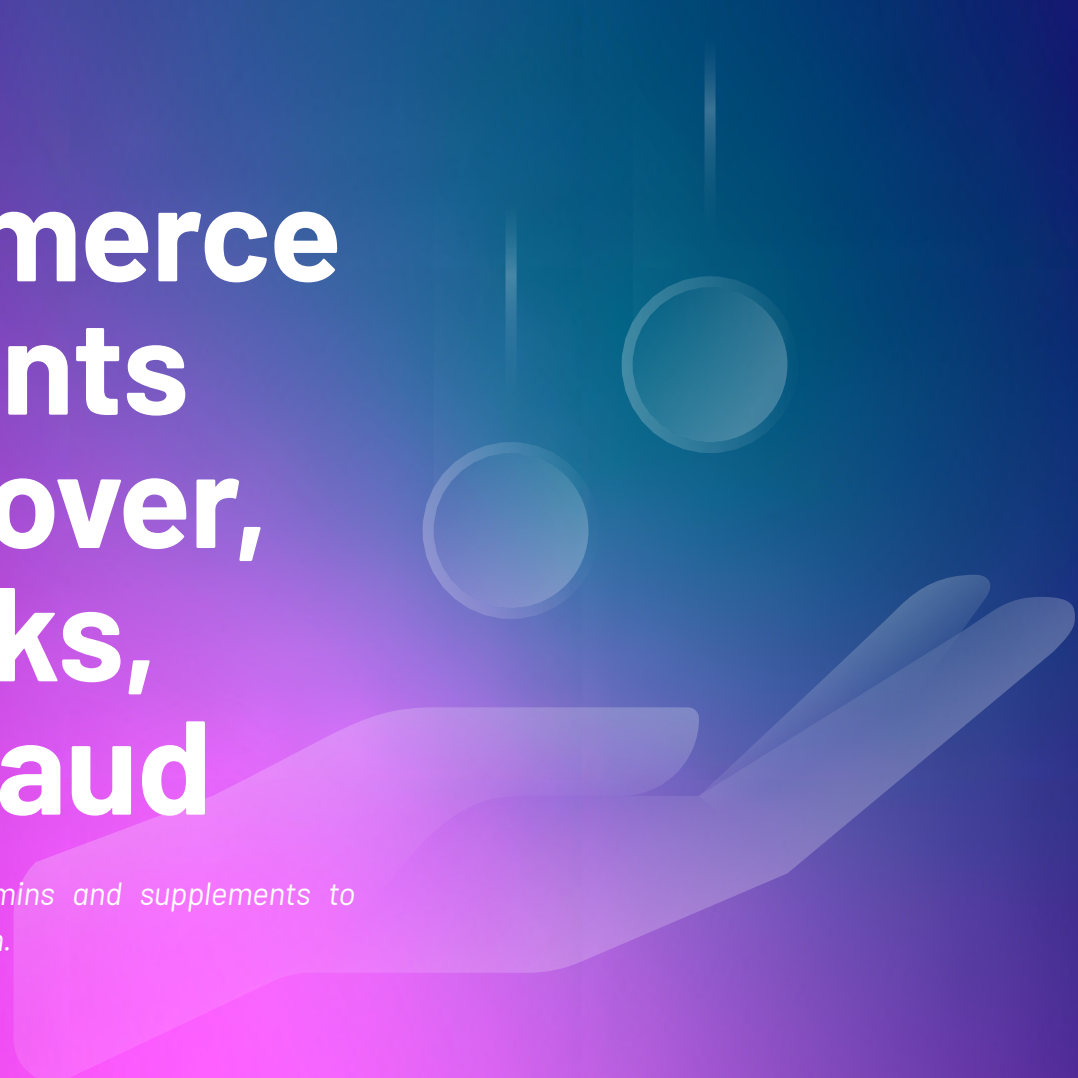
The following tips are a strong start:

- Encrypt or hash stored credentials on your website.
- Require rigorous password practices and multifactor authentication
- Proactively monitor compromised credentials to flag and prevent logins with stolen usernames and passwords.
- Adopt a behavior-based bot management solution to stop ATO attacks against your web and mobile apps and APIs.
- Continuously evaluate users' post-login behavior to determine if their activities within an account are legitimate.

[HUMAN Account Protection](#) provides a layered defense model to stop account takeover attacks at every turn. Our solutions work together to stop bot attacks in real time, reduce your potential attack surface area, and remediate breached accounts.

Global E-Commerce Retailer Prevents Account Takeover, Carding Attacks, and Review Fraud

This leading global e-commerce retailer distributes vitamins and supplements to customers globally through its website and mobile application.



Global E-Commerce Retailer Prevents Account Takeover, Carding Attacks, and Review Fraud

EDITOR'S NOTE

FAKE REVIEWS ARE A HOT TOPIC—AND HERE'S WHY

CRACKING DOWN ON FAKE REVIEWS

HOW HIGHER EDUCATION CAN COMBAT BAD BOTS, FAKE ACCOUNTS

SEVEN WAYS CYBERCRIMINALS COMMIT ACCOUNT FRAUD

GLOBAL E-COMMERCE RETAILER PREVENTS ACCOUNT TAKEOVER, CARDING ATTACKS, AND REVIEW FRAUD

HOW HUMAN CAN HELP

THE CHALLENGE

The retailer was experiencing a high volume of malicious bot traffic on its e-commerce portal, including account takeover (ATO), credential stuffing, and carding attacks. The company's security team was working around the clock to respond in real time.

Additionally, fraudsters were also using bots to post fake reviews and 'like' the reviews in order to take advantage of monetary incentives. Not only did this mean that attackers were rewarded for fake reviews, but it also compromised the authenticity of the website's reviews.

THE SOLUTION

The retailer needed a solution that would accurately identify and block malicious bot activity without affecting its user experience. [HUMAN Application Protection](#) was the clear choice.

Protection against ATO and carding attacks

With its sophisticated machine learning, Application Protection detects malicious behavior on websites in real time, stopping the most advanced bot attacks.

Product review monitoring

Application Protection applies the same learning techniques to predict when a product review or rating is likely to have been submitted by a bot and challenges the review before it is published.

Flexible architecture with easy integration

Application Protection's open architecture allows it to easily interface with any existing technology stack, including Amazon Web Services (AWS). Application Protection sits in front of the retailer's AWS instances and blocks malicious bot attacks before they reach the servers, without adding an additional layer of in-line traffic processing. This maintains performance and ensures low latency by reducing overall server load. Application Protection also seamlessly integrates with industry-leading CDNs, including Amazon CloudFront with AWS Lambda, to protect services hosted on AWS.

THE RESULTS

After implementing Application Protection as part of its multi-tier security strategy, the retailer experienced several benefits:

- **Dramatic drop in ATOs** and other malicious bot attacks, ensuring a safe shopping experience without adding friction to the customer journey
- **Significant reduction in fake reviews** being left on the company's product, restoring customers' confidence in using the website's reviews to inform purchasing decisions
- **Improved operational efficiency** because the team no longer had to spend time, money and other resources reactively responding to bot attacks

"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, Leading Global E-Commerce Retailer

EDITOR'S NOTE

FAKE REVIEWS ARE A HOT TOPIC—AND HERE'S WHY

CRACKING DOWN ON FAKE REVIEWS

HOW HIGHER EDUCATION CAN COMBAT BAD BOTS, FAKE ACCOUNTS

SEVEN WAYS CYBERCRIMINALS COMMIT ACCOUNT FRAUD

GLOBAL E-COMMERCE RETAILER PREVENTS ACCOUNT TAKEOVER, CARDING ATTACKS, AND REVIEW FRAUD

HOW HUMAN CAN HELP

How HUMAN Can Help

The HUMAN Defense Platform, including product suites Application Protection and Account Protection, helps combat these threats effectively. HUMAN technology safeguards institutions by blocking the automated creation of fake accounts and monitoring post-login activity for suspicious behavior, ensuring that your systems are secure and your resources are protected.



About HUMAN

HUMAN is trusted by the world's leading enterprises and internet platforms to prevent, detect, and respond to cyberattacks with unmatched scale, speed, and decision precision across their advertising, application, and account surfaces. Safeguard your customer journey end to end with complete confidence by consolidating with the Human Defense Platform. **To Know Who's Real**, visit humansecurity.com.



[Request a Demo](#)