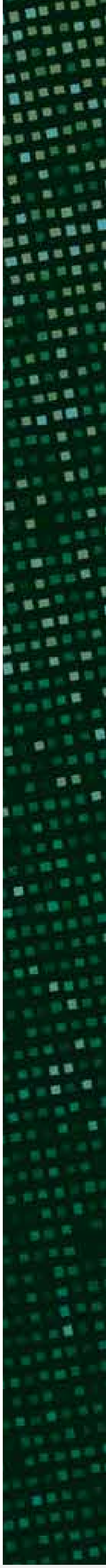
SPOOF 2023:

TRENDS IN ONLINE BRAND IMPERSONATION OF RETAIL, HOSPITALITY & CONSUMER BRANDS

ALLURE SECURITY

TABLE OF CONTENTS



EXECUTIVE SUMMARY

This report – Summary of Patterns & Observations in Online Fakes (SPOOF) 2023: Trends in Online Brand Impersonation of Retail, Hospitality & Consumer Brands – analyzes incidents of online brand impersonation affecting consumer-facing brands from **January** through **July 2023.**

Key Insights:

- Month-over-month, online impersonations of consumer-facing brands grew 29% in June and 44% in July
- Apparel (39.7%), Consumer Products (37%), and Travel (7.8%) are the most frequently impersonated brand categories
- More than half of scam websites (54%) don't immediately impersonate consumer-facing brands, highlighting the need for ongoing monitoring of suspicious domains
- Meta was the preferred social media platform for brand impersonation, with 82% of social media impersonations occurring on Facebook or Instagram
- The growing use of scam ads featuring a brand's assets on social media leads to cybersecurity, reputation, and fraud risk, and also diminishes digital marketing ROI
- Stricter enforcement by e-commerce giants like Amazon and eBay is driving fraudsters to build their own generic online storefronts for counterfeit goods or non-delivery scams
- Traditional domain-permutation-based detection methods would have missed 87% of retail brand impersonations; proving out the need for modern AI-powered approaches

Fraudsters' continued exploitation of consumer trust in consumer-facing brands leads to tarnished reputations, increased fraud, and eroded consumer confidence. The ongoing threat also undermines marketing investments, and fraudsters' continued cloaking innovations (i.e., detection avoidance) render traditional online brand protection methods obsolete.

There's an urgent need for retail, hospitality and other consumer-facing brands to modernize their brand protection programs and technology to counter this escalating threat.

INTRODUCTION

Welcome to Allure Security's inaugural report on online brand impersonations of retail, hospitality, and other consumer-facing brands. As far as we know, this is the only annual report that delves specifically into online impersonations across retail sectors including apparel, consumable and durable consumer goods, travel, hospitality, consumer services, e-commerce marketplaces, automotive, food service/restaurants, and entertainment.

From January through July 2023, our AI-powered engine examined billions of digital assets in total, exposing thousands of impersonations of consumer-facing brands. This report offers a comprehensive analysis of these impersonation attacks to shed light on emerging trends and provide actionable insights. We set out to help consumer-facing brands more effectively protect their brand, customers, and potential customers more effectively online.

Furthermore, if you're not yet convinced, we hope to demonstrate that online brand impersonation attacks have far-reaching implications beyond just your cybersecurity, fraud, brand protection, or legal team. They also undermine the performance of digital marketing campaigns. Marketing dollars don't go as far on diluted online channels cluttered with fraudulent ads or deceptive websites rising up in search engine results.

Finally, traditional online brand protection methods can no longer match the evolving tactics of fraudsters and their techniques for escaping detection. Now is the time for all brands to invest in AI-powered brand protection to combat these escalating challenges.

METHODOLOGY & DATA SOURCES

Allure Security's AI-powered brand impersonation detection engine employs machine learning, image analysis, and natural language processing to analyze millions of digital assets daily. With this SPOOF23 report we focus specifically on brand impersonations of retail, hospitality and other consumer-facing brands from January 1 through July 31, 2023.

Content analyzed by our AI models come from a multitude of sources, including:

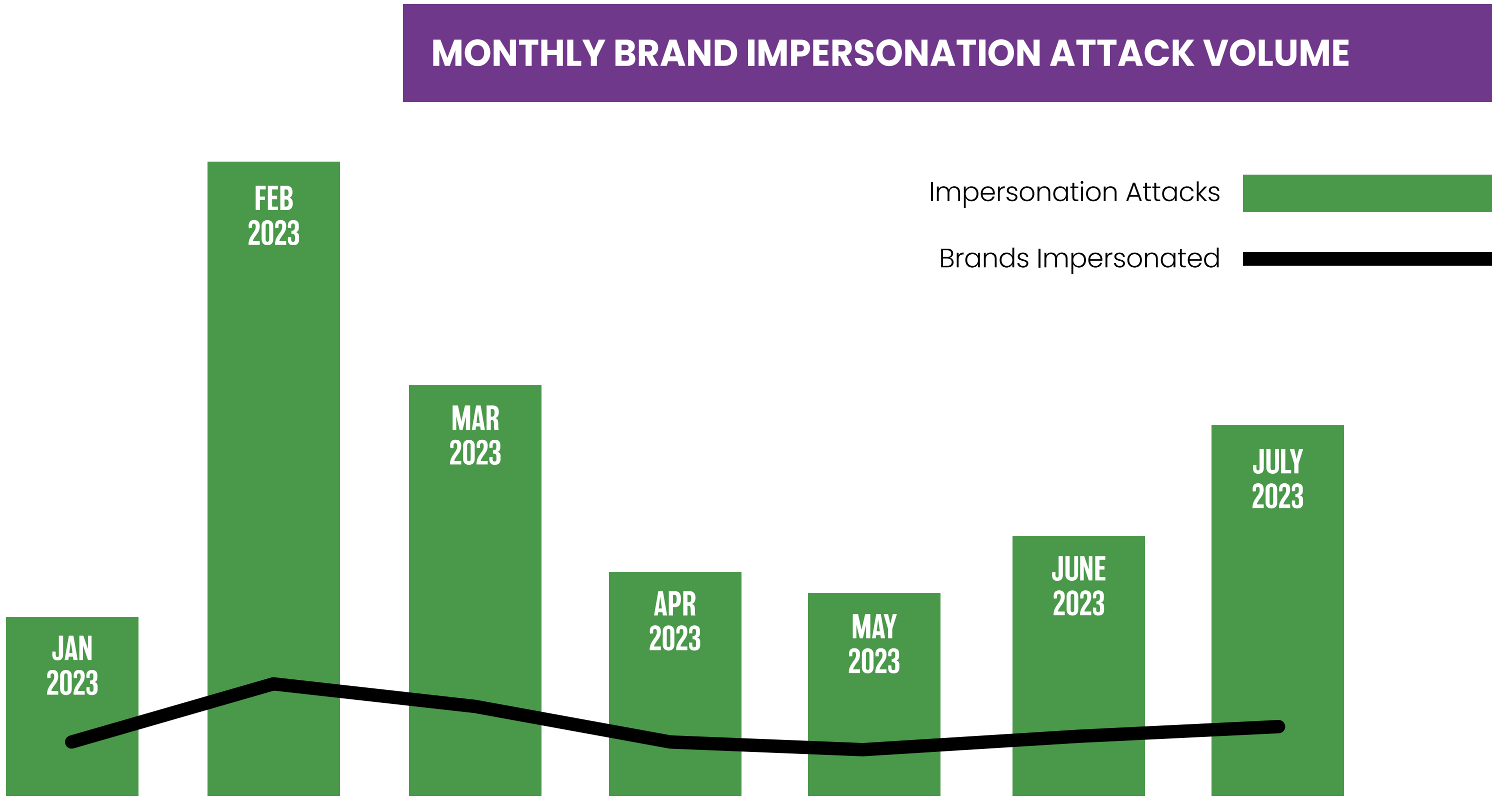
- New and dormant domains & sub-domains (all global TLDs)
- Allure Security signals, referrer logs, and threat research inputs
- Social media profiles
- Mobile app marketplace listings
- Online ad URLs
- Threat intel feeds

A unique capability of our brand protection service is ongoing, automated monitoring of digital assets such as URLs, social media profiles, and mobile app marketplaces. This capability allows us to track the age of websites that end up impersonating a brand. Not all brand threats materialize as impersonations as soon as they go live on the internet. For further details, refer to the report's "Average Spoof Gestation Period" section.

Our technology and services enable us to conduct frequent, thorough analysis of online content for impersonations of the brands we monitor. However, the sheer size of the internet makes it impossible to monitor everything. As a result, this report likely under-reports the full extent of the problem, especially for retail, hospitality, and consumer-facing brands that are not yet Allure Security customers. Our customers enjoy enhanced visibility thanks to more extensive large-data model training and AI-powered monitoring tailored to their brands.

SPOOFS OF CONSUMER-FACING BRANDS ONLINE IN 2023

MONTHLY BRAND IMPERSONATION ATTACK VOLUME: FROM POST-HOLIDAY SLUMP TO MID-YEAR INCREASE



The graph above charts the trend of online impersonations of consumer-facing brands we detected each month along with the number of brands impersonated. During the reporting period, 56% of consumer-facing brands were impersonated more than once and some highly targeted brands were impersonated hundreds of times within a single month.

The smaller number of online impersonations in January 2023 reflects the usual post-holiday slump in e-commerce. The February surge might be attributed to fraudsters exploiting opportunities around Valentine's Day to lure shoppers with steep discounts on luxury items. Promotions tied to the Super Bowl or President's Day also drive more people to shop online in February, offering fraudsters more potential victims. Impersonations then dropped from March to May, but grew 29% in June and another 44% in July month over month.

APPAREL & OTHER CONSUMER PRODUCTS ARE THE MOST IMPERSONATED BRAND CATEGORIES

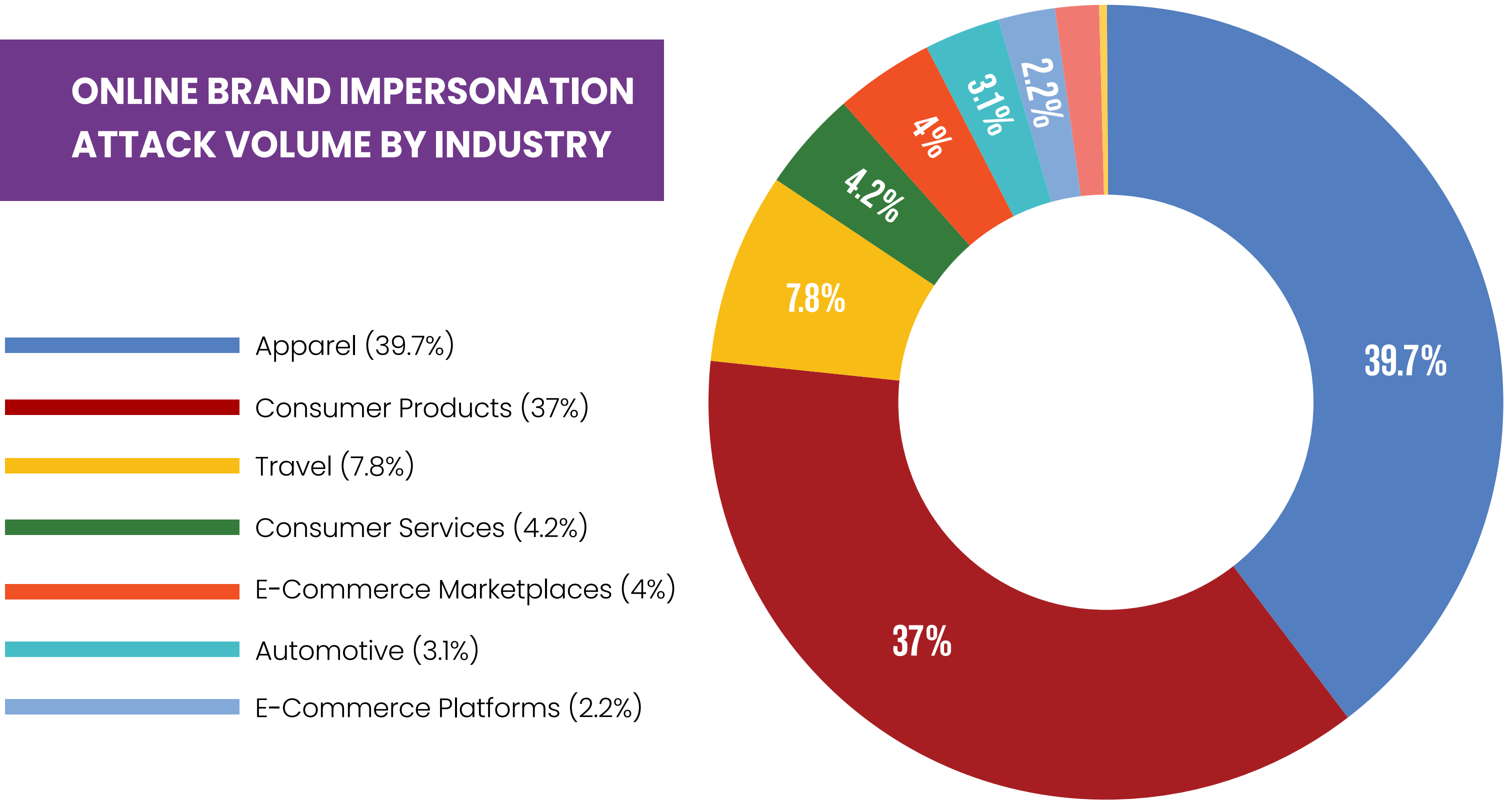
We analyzed online impersonations of consumer-facing brands from January 1 to July 31, 2023 and categorized them into nine sub-groups:

- Apparel
- Consumer products (consumable & durable)
- Travel & hospitality (not including restaurants)
- Consumer services
- E-commerce marketplaces
- Automotive
- E-commerce platforms
- Food service / Restaurants
- Entertainment

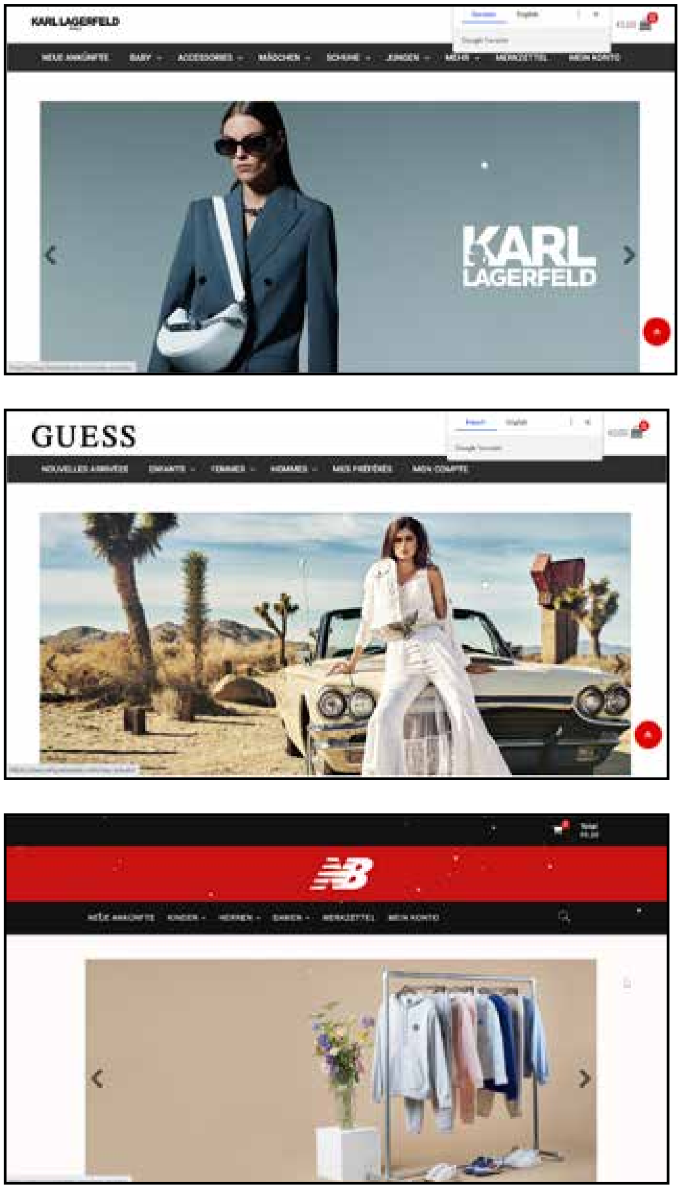
APPAREL & OTHER CONSUMER PRODUCTS ARE THE MOST IMPERSONATED BRAND CATEFORIES

In the reporting period, the most frequently impersonated categories were Apparel accounting for 39.7% of all impersonations, Consumer Products at 37%, and Travel with 7.8%.

ONLINE BRAND IMPERSONATION ATTACK VOLUME BY INDUSTRY



It's important to note that fraudsters rely less and less on using variations of a brands' authentic domain name for impersonation. They know many brands and vendors iterate domain permutations to detect impersonations. In fact, traditional detection methods based on domain permutations would have failed to recognize 87% of the retail or consumer-facing impersonations detected by Allure Security's automated, AI-based analysis of millions of online artifacts each day.


KARL LAGERFELD
NEUE ANKÜNFTE BABY ACCESSOIRES MÄDCHEN SCHUHE JUNGEN MEHR MERKZETTEL MEIN KONTO
KARL LAGERFELD
GUESS
NOUVELLES ARRIVÉES ENFANTS FEMMES HOMMES MES PRÉFÉRÉS MON COMPTE
NB
NEUE ANKÜNFTE KINDER HERREN DAMEN MERKZETTEL MEIN KONTO

An example of a cloaking technique fraudsters use to circumvent permutation-based detection is using seemingly random first and last name combinations as their domain name (e.g., FatmaAlaloaoui.com, VickyNakanishi.com, EvaGunther.com), while impersonating fashion and footwear brands like Karl Lagerfeld, Guess, and New Balance. Conventional detection methodologies that typically only look at the URL, maybe the page title, and sometimes copyright information would overlook these impersonations. What's required is more advanced AI-powered detection that doesn't focus solely on certain keywords. Instead, a detention engine needs to inspect a web page in its full context, examining multiple elements including imagery, text, and code to take a more holistic view – much like a human evaluator would.

SCREENSHOTS OF FATMALALAOUI.COM, VICKYNAKANISHI.COM, AND EVAGUNTHER.COM IMPERSONATING KARL LAGERFELD, GUESS, AND NEW BALANCE RESPECTIVELY

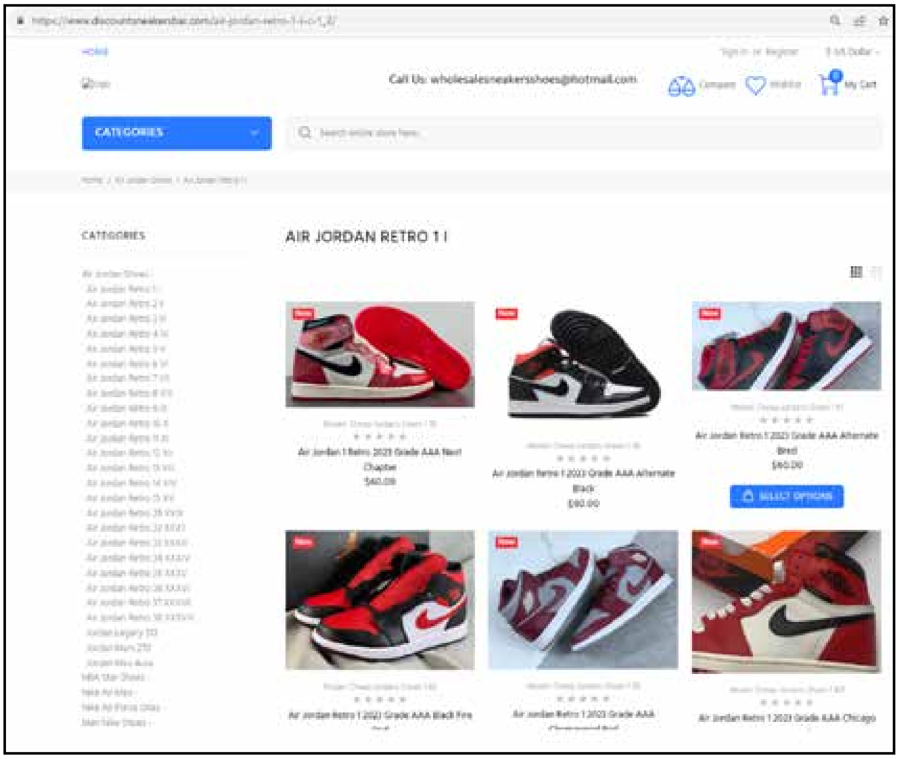
EMERGING:

THE RISE OF GENERIC ONLINE SCAM STOREFRONTS

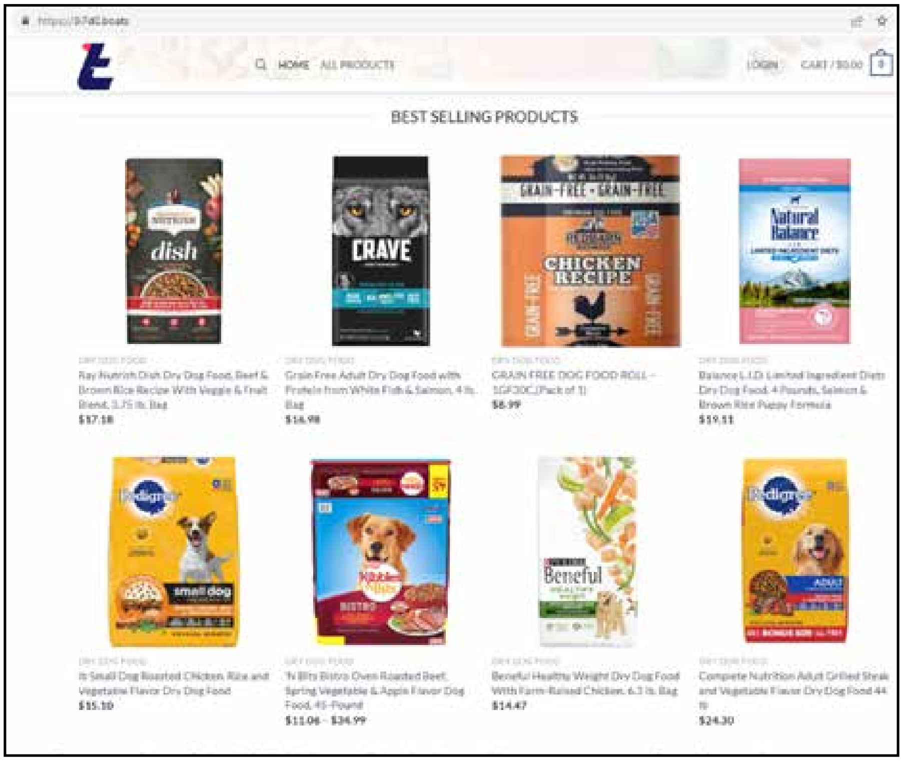
We've observed an increase in generic online scam shops offering various consumer goods – footwear, apparel, and appliances in particular. This emerging trend is gaining traction. Typically fraudsters lure victims to these online scam shops using online ads that offer incredible discounts.

E-commerce companies like Amazon and eBay are trying to step up their efforts to crackdown on counterfeit listings with Amazon's Brand Registry Program and eBay's Verified Rights Owner Program. It appears Amazon and eBay are making it harder for scammers to do business on their marketplaces. In response, we see fraudsters pivoting.

Increasingly, some fraudsters use generic online storefronts they create themselves in order to partake in non-delivery fraud (where a victim pays for goods but never receives them) or the sale of knock-offs. These shops don't mimic established e-commerce sites. Instead they simply use a generic brand and market a mix of goods from various brands without directly impersonating any of them.


HOME
Call Us: wholesalesneakersshoes@hotmail.com
Compare
Wishlist
My Cart
CATEGORIES
CATEGORIES
AIR JORDAN RETRO 1 I
Air Jordan 1 Retro 2023 Grade AAA Next Chapter
$60.00
Air Jordan Retro 1 2023 Grade AAA Alternate Black
$60.00
Air Jordan Retro 1 2023 Grade AAA Alternate Bred
$60.00
SELECT OPTIONS
Air Jordan Retro 1 2023 Grade AAA Black Fire
Air Jordan Retro 1 2023 Grade AAA
Air Jordan Retro 1 2023 Grade AAA Chicago

SCREENSHOT OF THE "DISCOUNTSNEAKERSBAR.COM" WEBSITE AND ITS CATALOG OF SIGNIFICANTLY DISCOUNTED AIR JORDAN 1S.



https://3i7d0.boats

BEST SELLING PRODUCTS

DRY DOG FOOD
Ray Nutrish Dish Dry Dog Food, Beef & Brown Rice Recipe With Veggie & Fruit Blend, 3.75 lb. Bag
$17.18

DRY DOG FOOD
Grain Free Adult Dry Dog Food with Protein from White Fish & Salmon, 4 lb. Bag
$16.98

DRY DOG FOOD
GRAIN FREE DOG FOOD ROLL – 1GF30C (Pack of 1)
$8.99

DRY DOG FOOD
Balance L.I.D. Limited Ingredient Diets Dry Dog Food, 4 Pounds, Salmon & Brown Rice Puppy Formula
$19.11

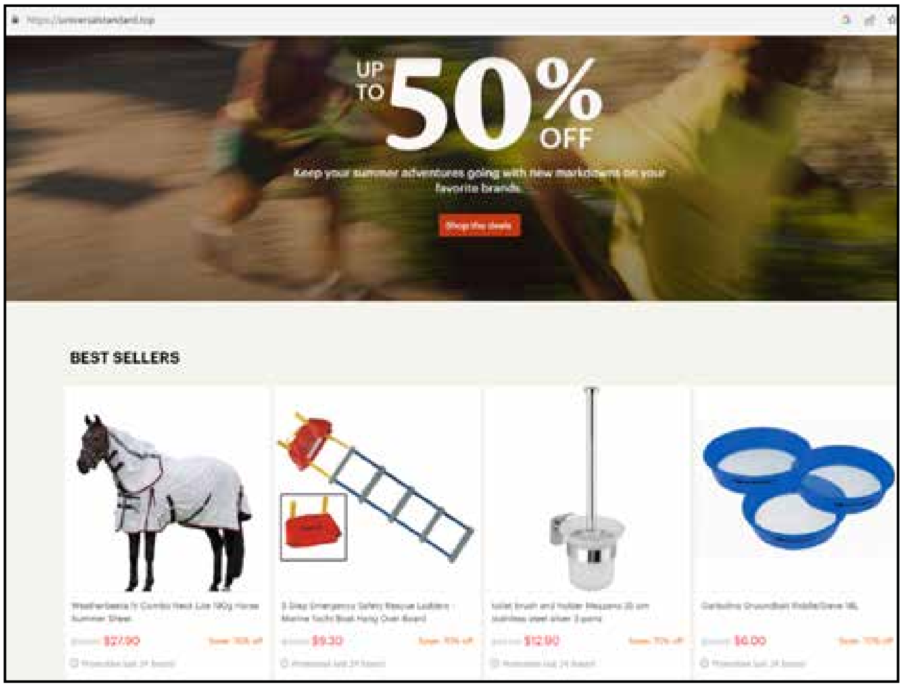
DRY DOG FOOD
ts Small Dog Roasted Chicken, Rice and Vegetable Flavor Dry Dog Food
$15.10

DRY DOG FOOD
'N Bits Bistro Oven Roasted Beef, Spring Vegetable & Apple Flavor Dog Food, 45-Pound
$11.06 – $34.99

DRY DOG FOOD
Beneful Healthy Weight Dry Dog Food With Farm-Raised Chicken, 6.3 lb. Bag
$14.47

DRY DOG FOOD
Complete Nutrition Adult Grilled Steak and Vegetable Flavor Dry Dog Food 44 lb
$24.30

SCREENSHOT OF THE "3I7D0.BOATS" WEBSITE SELLING VARIOUS PET FOOD BRANDS



https://universalstandard.top

Keep your summer adventures going with new markdowns on your favorite brands.

BEST SELLERS

WeatherBeeta [illegible] Combo Neck Lite 190g Horse Summer Sheet
[illegible] $27.90 Save 70% off
[illegible]

3 Step Emergency Safety Rescue Ladder Marine Yacht Boat Hang Over Board
[illegible] $9.30 Save 70% off
[illegible]

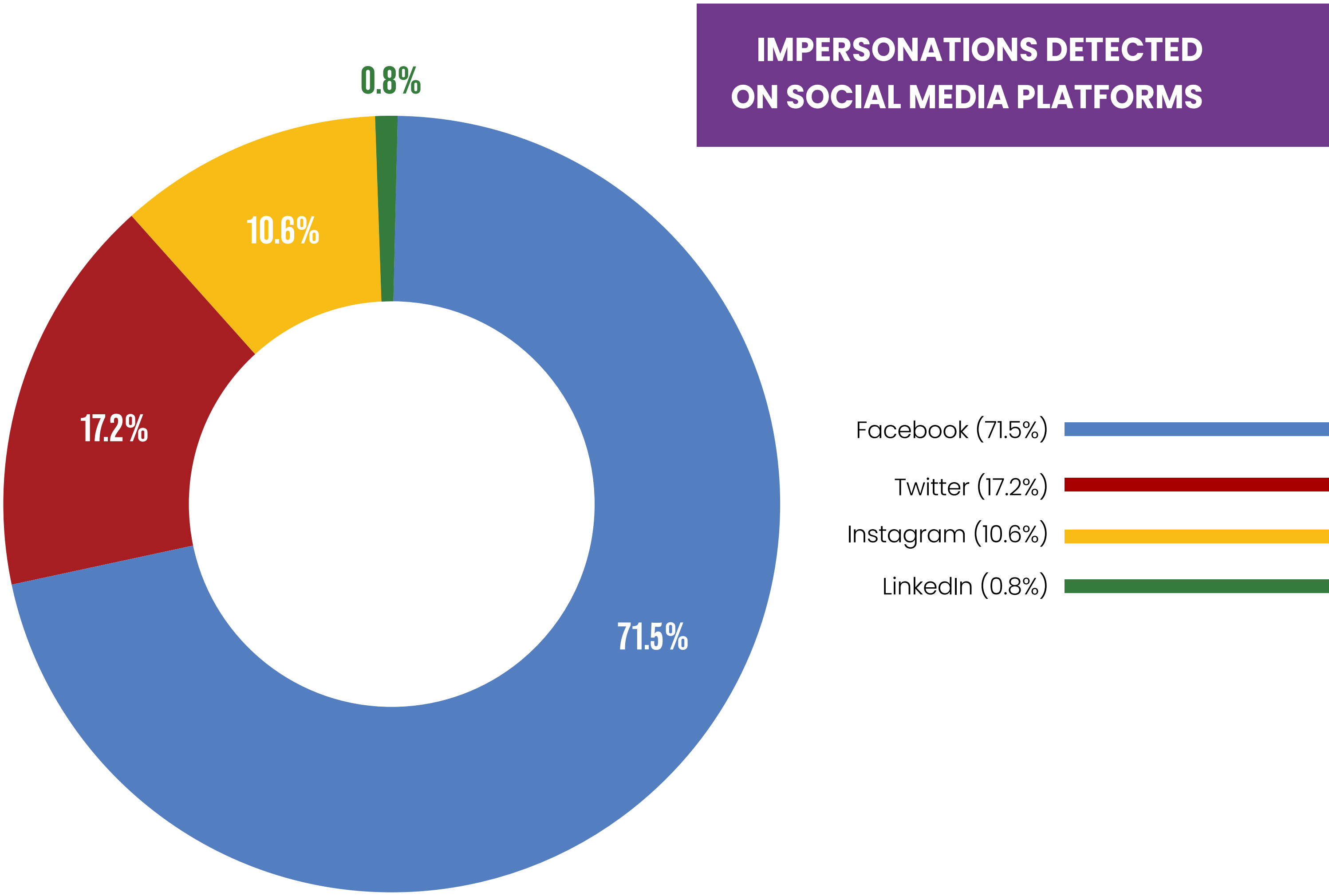
toilet brush and holder [illegible] 35 cm stainless steel silver 3 parts
[illegible] $12.90 Save 70% off
[illegible]

[illegible] 18L
[illegible] $6.00 Save 70% off
[illegible]

SCREENSHOT OF THE "UNIVERSALSTANDARD.TOP" WEBSITE OFFERING PRODUCTS FROM HORSE CLOAKS TO TOILET BRUSH HOLDERS

We've seen examples of these scam shops focusing on jewelry and various jewelry brands, footwear and multiple shoe brands, or offering an eclectic mix of products such as industrial supplies alongside food products.

BRAND IMPERSONATIONS ON SOCIAL MEDIA — FACEBOOK LEADS THE PACK



IMPERSONATIONS DETECTED ON SOCIAL MEDIA PLATFORMS

The chart illustrates the distribution of online brand impersonations detected by Allure Security on Facebook, Twitter, Instagram, and LinkedIn. Impersonations of consumer brands on LinkedIn were less prevalent in our data set based on LinkedIn's business-centric nature.

Our analysis reveals that the majority of social media impersonations of consumer brands occurred on Facebook. Meta's downsizing of its online trust and safety teams earlier this year is a likely contributor to this growing issue. Many of these impersonations took the form of deceptive ads promising extraordinary discounts. Consumer goods topped the list at 57% of Facebook impersonations, and included items such as gift cards, consumer packaged goods, and household appliances. Apparel brands followed at 18% of impersonations on Facebook and include footwear, clothing, jewelry, and more. Travel brands came in third at 12% of Facebook impersonations and spanning airlines, travel-booking platforms, and hotels.

In the first seven months of 2023, we observed the second-highest number of social media impersonations on X (formerly Twitter) at 17%. In most cases, these impersonations took the form of fake profiles that included the target company's brand name and logo but little to any additional content or activity. The fraudsters' intentions for these fake profiles remain unclear. They could have been aging the profiles in order to increase their credibility/ believability and/or preparing to directly message Twitter users that mentioned the impersonated retail brand.

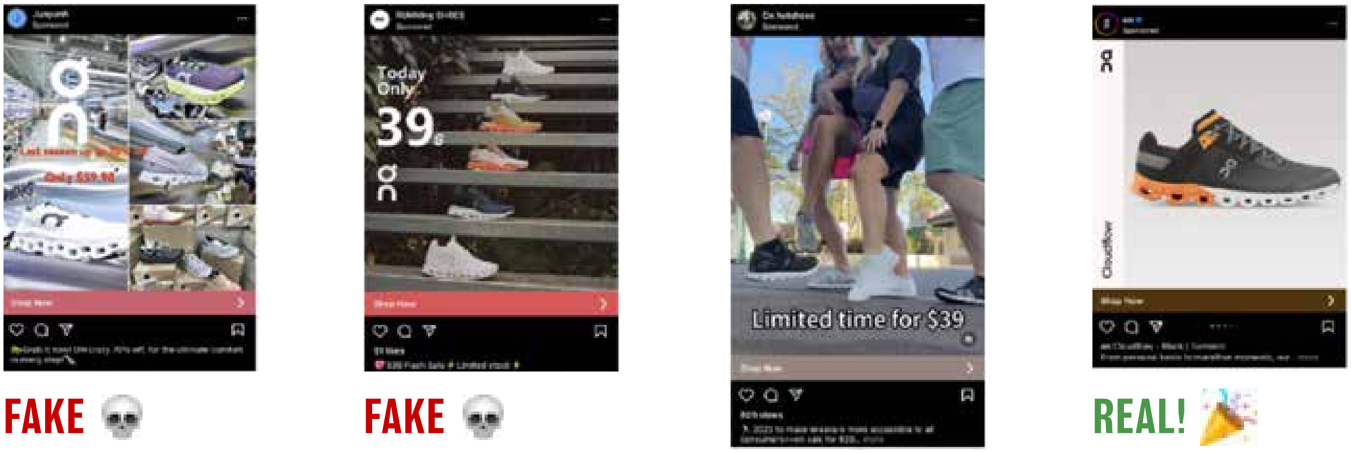
Instagram takes third place for prevalence of brand impersonations detected by Allure Security on social media. Many of these impersonations involved fake ads promoting steep discounts on consumer goods and apparel. While outside of the reporting period for this report, we continue to observe an increase in fraudsters' use of deceptive ads on Instagram. See the "Meta Ads - Haystack of Deceit?" write-up below for more.

EMERGING:

META ADS – HAYSTACK OF DECEIT?

We've observed an increase in scammers using ads on Facebook and Instagram to promote steep discounts on apparel and directing to scam websites. As an example, Instagram recently served an Allure Security investigator three fraudulent ads for a popular running brand he'd been researching before he was presented with a genuine ad from the legitimate brand. The genuine ad was a needle at the bottom of a haystack of deceit.

Not only do these ads place consumers at risk, they damage a brand's reputation and marketing return-on-investment. An influx of counterfeit ads means marketers have to compete with fraudsters for their same ad keywords. Additionally, as in the example illustrated below, the fraudulent ads push legitimate ads out of view. They also create a scenario where consumers are more likely to be lured by a scam ad than see a legitimate ad from the authentic brand.



AD 1 FAKE 💀

AD 2 FAKE 💀

AD 3 FAKE 💀

AD 4 REAL! 🎉

SCREENSHOTS OF THREE SCAM ADS FOLLOWED BY ONE GENUINE AD DISPLAYED IN CHRONOLOGICAL ORDER TO AN INSTAGRAM USER

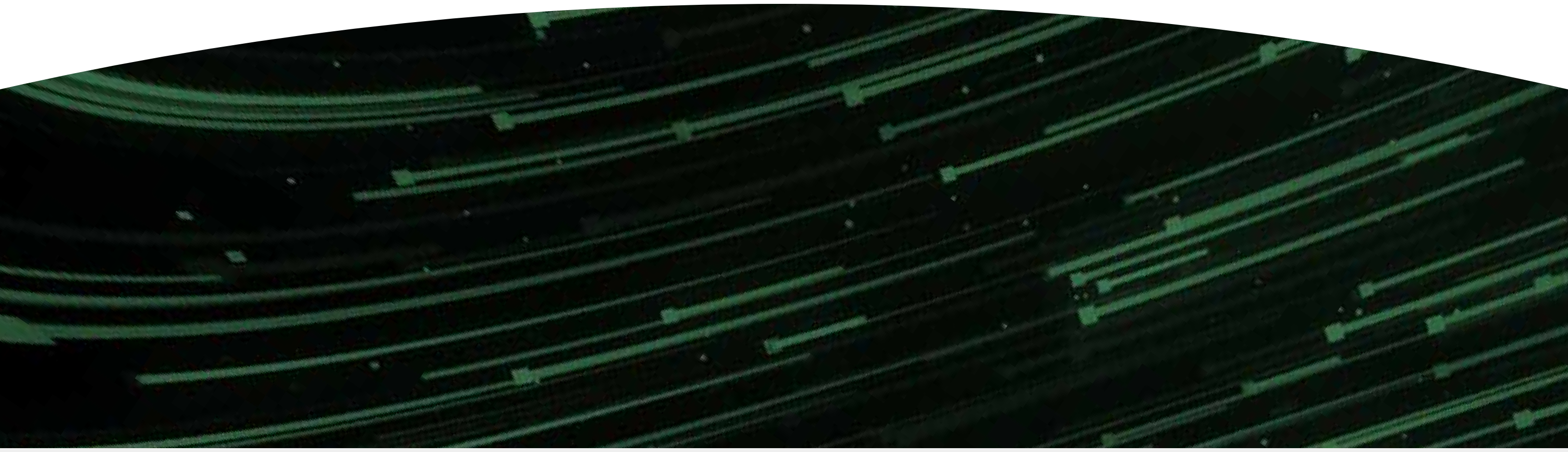
Most scam ads identified by Allure Security on Facebook and Instagram target apparel and durable consumer-goods brands and promote steep discounts. Additionally, many of the destination fake sites will only display on mobile devices – likely a tactic taken to avoid primitive detection methods.

These scam ads tend to fall into four categories:

- Ads directing victims to scam websites impersonating the brand's website
- Ads directing victims to scam websites impersonating other legitimate retailer brands (e.g., Dick's Sporting Goods, DSW, and Nordstrom Rack) marketing goods from numerous brands
- Ads directing victims to purchase consumer goods and apparel through Facebook Messenger or WhatsApp
- Ads directing victims to generic online scam shops marketing goods from numerous brands (see "The Rise of Generic Online Scam Storefronts" above)

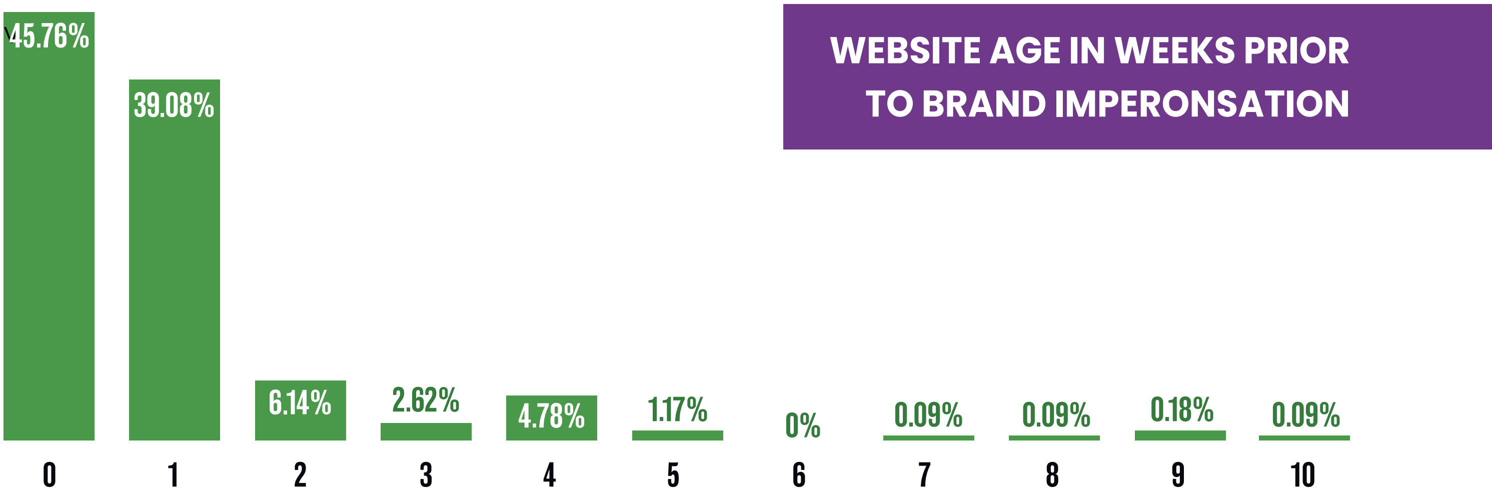
Scammers' objectives with these schemes are to profit by selling counterfeits, engaging in "non-delivery fraud" where consumers pay for goods they never receive, selling victims' financial information, or other forms of identity theft.

When Allure Security facilitated the takedown of ads (i.e., for Allure Security customers), associated websites quickly changed their content to impersonate different apparel brands or retailers or showcase different products. This quick action in response to discovery suggests scammers used automated tools that allow them to develop, test, and launch ad variations rapidly and then update corresponding scam websites in real time.



COUNTDOWN TO DECEPTION: AVERAGE SPOOF GESTATION PERIOD

With our unique AI-powered detection methodology, we don't inspect a domain just once. We continually revisit domains to identify any threat as soon as there is a signal that it's developing into a threat. We flag a domain for surveillance when it presents just a single indicator that matches any artifacts associated with a brand we monitor, even if there's not yet enough evidence to qualify as an impersonation. For example, a page title may include "Super Duper Shoes," but absent any additional suspicious content, it doesn't necessarily signal intent to impersonate Super Duper Shoes.



Our data shows that less than half (45.76%) of the domains we flag immediately impersonate a consumer-facing brand when they first appear on the internet (represented as week zero in the chart). The majority of flagged domains either start with no content (e.g., parked domains) or content that seems harmless. Another 39.08% of domains we flagged transformed into brand impersonations within their first one-to-seven days. At the extreme, some websites that end up becoming brand impersonations lie dormant for more than two months (10 weeks) after we begin tracking them.

Fraudsters are capitalizing on the insurmountable amount of work brands face using traditional methods of reviewing a list of hundreds of domain name permutations daily, and then also constantly visiting those websites day after day to see whether they've become a threat. Our findings highlight the limitations of single point-in-time examinations of suspicious domains. Persistent AI-powered monitoring is imperative to eliminating impersonation threats pro-actively – the moment they become malicious and before they harm a single consumer.

A NEW ERA OF HOPE FOR ONLINE BRAND PROTECTION

Historical approaches to finding online brand impersonations, like searching for domain name variations or waiting for victims to report them are no longer adequate in today's world. Adversaries have adapted, making methods based solely on lookalike domain names mostly ineffective – catching a mere 10 to 13% of today's spoofs.

Before automated, AI-powered detection like Allure Security's, it was too difficult to inspect the incredible volume of online content. Old methods focused on domain name permutations to make the task manageable.

With Allure Security's AI-powered approach, however, we can monitor online content both more broadly and deeply – looking at numerous indicators beyond just the URL. We don't focus on, nor even really care about, the URL of a website. Through our large-data model training, we understand how legitimate brands go to market so we can spot impersonations regardless of their domain name.

If you're ready to detect brand impersonations more accurately and quickly (and before your customers do), achieve more successful takedowns, and significantly reduce time-to-takedown, get in touch with Allure Security today.

ABOUT ALLURE SECURITY

Allure Security online brand protection-as-a-service automates the examination of more of the digital world with AI – millions of online assets each day including domains, online ads, social media posts and profiles, and mobile app product pages.

Consequently, and compared to alternatives, Allure Security identifies more online brand impersonations more quickly and closer to their first appearance on the internet — before a single human sees or falls victim to a digital imposter.

Finally, Allure Security's best-in-class takedown service and unique three-pronged approach to response – blocklisting, decoy data, and takedown diligence – increases takedown success rates and reduces time to takedown.

Deploying Allure Security allows brands to strengthen online reputation, customer trust, and customer satisfaction, as well as: reduce fraud, lost sales, customer churn, customer complaints, and staff burnout.

PHONE
877-669-8883

E-MAIL
info@alluresecurity.com

LINKEDIN
https://www.linkedin.com/company/alluresecurity

TWITTER
https://twitter.com/alluresecurity

ALLURE

SECURITY