FORTRA™

GUIDE (PHISHLABS)

Disrupt Counterfeit Threats

Online counterfeit attacks targeting ecommerce have more than tripled in quantity in the last decade, reaching $5 trillion in losses to the global economy annually. Counterfeit campaigns redirect sales and compromise consumer data using brand recognition, the same component critical to driving legitimate online sales. Attackers incorporate stolen designs and trademarks into counterfeit sites, outbid legitimate businesses with fraudulent advertisements, and impersonate brands and their executives with bogus social media accounts.

The massive expansion of ecommerce and online consumer-to-business interaction creates a complex attack surface difficult for security teams to navigate. As buying behavior is increasingly driven by online relationships between consumer and brand, protecting your digital presence is critical.

This playbook will give security teams a better understanding of:

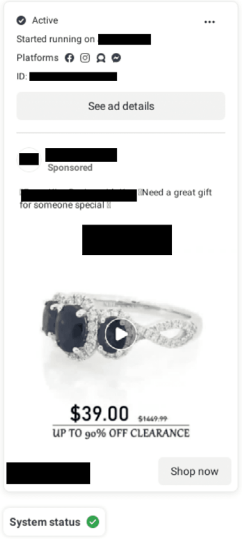
- The four most common types of counterfeit activity
- How to collect intelligence on counterfeit threats, and
- Strategies to curate and mitigate counterfeit threats.

Common Types of Counterfeit Activity

Fraudulent Advertisements

Sponsored advertisements on social media promote fake products, redirect traffic to counterfeit websites with a malicious or spoofed link, and drive ad prices for legitimate organizations. Sponsored ads are created via falsely branded business accounts and use stolen copy, imagery, and a strong call to action, like a flash sale, that plays to consumer emotions. Threat actors can tailor these ads to the audience of their choice and determine the budget and duration of their attack.

As fraudulent advertisements grow in popularity, legitimate organizations are finding themselves forced to compete directly with criminals for advertising space. Fraudulent advertisements populated through Google search are also targeting businesses on the open web. These malicious advertisements have a low-cost barrier to entry and abuse geofencing to target victims.



Active

Started running on [redacted]

Platforms

ID: [redacted]

[redacted]

Sponsored

[redacted] Need a great gift for someone special

[redacted]

[redacted]

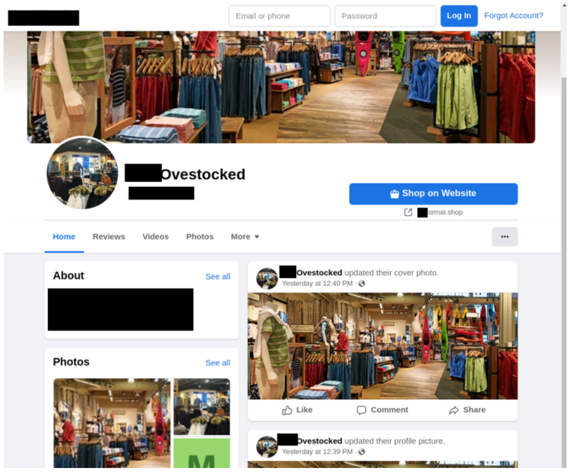
Fraudulent Advertisement

Unauthorized Account Pages on Social Media

The rise in social commerce has positioned a business's social media presence as a key differentiator among competitors, and misinformation or brand abuse can have permanent negative consequences to an organization's reputation or bottom line.

Threat actors are taking advantage of investments in brand-btuilding and consumer engagement via social platforms to create phony account pages. Brand abuse on social media encompasses the unauthorized use of copyrighted material, trademarks, and other IP to create fake account pages and advertisements.

The volume of unprotected data and ease of account creation makes mimicking account pages an undemanding operation for threat actors. Additionally, impersonation enhances the credibility of the fake site and aids in its ability to avoid detection.



[redacted]

[redacted]Ovestocked

[redacted]

[redacted]ormal.shop

About

[redacted]

[redacted]Ovestocked updated their cover photo.
Yesterday at 12:40 PM

[redacted]Ovestocked updated their profile picture.
Yesterday at 12:39 PM

Brand Impersonation

Counterfeit Sites

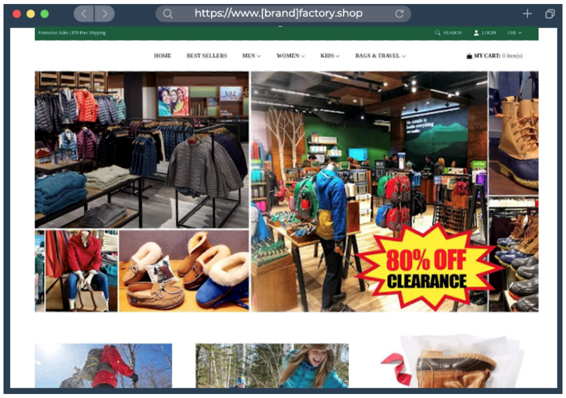
Online storefronts on the open web mimic reputable brands by using look-alike domains, misleading copy, and stolen intellectual property. Common characteristics of a counterfeit site include:

Name of company, product, or industry term in the domain

- Logo of the legitimate organization
- Colors, branding, and images scraped from the legitimate website
- Sales terms associated with the brand

Actors are also integrating trusted payment applications such as PayPal to conduct seemingly reputable transactions and enhance the site's overall sense of legitimacy.

Additionally, email phishing lures and falsely branded pay-per-click lures on social media play a significant role in convincing victims they are interacting with a legitimate website.



https://www.[brand]factory.shop

Promotion Sales | $70 Free Shipping

MY CART: 0 item(s)

Counterfeit Website

Look-Alike Domains

Malicious domains serve as the foundation for a wide range of threats to businesses. Threat actors can easily stand up a look-alike domain, tailor it to their target, and launch a variety of campaigns including phishing emails and counterfeit websites. Threat actors also incorporate malicious domains into fraudulent ads and pages on social media to redirect consumers to counterfeit sites.

Look-alike domains are incredibly effective because they can leverage the brand reputation of the legitimate company or product. Domains can impersonate a brand the following ways:

TLD swap	phishlabs.tech	**Omission**	phshlabs.com
Subdomains	phish.labs.com	**Transposition**	phsihlabs.com
Typosquatting	phishlavs.com	**Insertion**	phishxlabs.com
Hyphenation	phish-labs.com	**Homoglyph**	phishlaƅs.com
Repetition	phishllabs.com	**Vowel-swap**	phishlebs.com
Replacement	ph1shlabs.com	**Addition**	phishlabss.com

How to Collect Intelligence on Counterfeit Threats

Organizations should continuously monitor profiles, posts and ads, newly registered domains, and open source third party sites for abuse of their brand. Large amounts of this data are typically accessible via APIs, and security teams should ensure they have the appropriate infrastructure to store what is captured. Not all sources are free, and each should be evaluated to determine whether the quality and timeliness of the data is worth incorporating into your anti-counterfeit budget.

Fraudulent Advertisements

Stolen trademarked materials are continually substituted or modified on counterfeit ads to appear generic and avoid timely identification/takedown. These ads evade detection by using imagery scraped from legitimate websites, but do not include brand-owned materials like logos. As a result, these ads may still be recognizable as the targeted retail brand, but lack the evidence needed to qualify for brand infringement on the platform.

Detection of fraudulent activity requires the continuous monitoring of digital advertisements on relevant social platforms using a combination of automation and human analysis. Identification of malicious ads should begin with automated searches within the platform's ad library using exact and fuzzy matching of brand-specific key terms and meta descriptions.

The logos, copy, and imagery of each suspicious advertisement should be inspected for misleading or unauthorized information by expert analysts specializing in both the retail brand and the platform through which the suspicious ad is displayed. The ad URL should also be examined to identify whether the domain is legitimate or spoofed using brand key terms.

Security analysts specializing in the brand should be prepared to manually search large volumes of potential abuse for suspicious imagery and content on newly created advertisements.

Unauthorized Account Pages on Social Media

To create a fraudulent advertisement on social media, threat actors typically first create or compromise an abandoned account on that platform. While large volumes of these accounts overtly use stolen imagery and copy, many are abandoned pages lacking identifiable branding that could be flagged as fraudulent. To prevent brand abuse and fraudulent ad creation through these pages, security teams need to distinguish between legitimate, mimicked, and compromised accounts.

A combination of technology and expert human analysis should be used to detect a page tied to a malicious advertisement. Automated searches within the space should continuously monitor for pages using key brand-related terms.

Security teams should manually search social profiles abusing their organization by monitoring for exact and fuzzy mentions of the brand and proprietary terms. They should also monitor for materials scraped from their legitimate website that may lack explicit mentions of the retail brand. Analysts specializing in both the brand and social platform should inspect each page for unauthorized logos, trademarked material, and copy.

Counterfeit Websites & Look-alike Domains

Fraudulent advertisements typically redirect victims to counterfeit storefronts on the open web. These sites use look-alike domains, unauthorized content, and stolen imagery to convince victims of their legitimacy and to conduct malicious activity. To detect and evade counterfeit sites, security teams should use a combination of automated technology, like crawlers, and human review, actively monitoring the open web for abuse of intellectual property, unauthorized association by third parties, and traffic diversion using your brand name.

Counterfeit sites often use look-alike domains to impersonate a targeted organization's legitimate webpage. Security teams should continuously monitor for domains impersonating their brand by consuming URL data available through:

- Domain registrars
- SSL transparency logs
- Active DNS queries
- Passive DNS data

Analysts should then pivot from confirmed malicious domains to uncover additional threats with manual review of the domain to identify other domains on the same IP. From there, related IP addresses and name servers can reveal threats associated with the initial fraud. If domains linked to the original threat do not contain content, they cannot be submitted for mitigation and must be monitored for any future content changes.

Automated and analyst anti-evasion techniques should be established to collect content, as threat actors seek to restrict access to security teams by way of user-agent blocking and screen size or viewport device restriction.

Strategies to Curate and Mitigate Counterfeit Threats

Once suspicious activity has been identified, scoring techniques should be implemented to refine the data collected. This will enable security teams to refine flagged items to those that represent your brand and distinguish legitimate threats from benign activity.

Scoring should be based on the search terms you want to identify and are relevant to your brand. Effective scoring will still result in large amounts of data and false positives, and to fully vet results, analysis should be conducted through a combination of machine and human review. Once unauthorized use of the brand is verified, its severity should be assessed.

It is essential that only relevant, actionable data be sent to providers for takedown. If a provider is frequently receiving false positives, they will consider your submissions junk, and you may be blocked.

Effective Mitigation

The broad scope of counterfeit campaigns and unclear boundaries of abuse make it challenging to remove online threats targeting brands. In order to effectively mitigate counterfeit threats, security teams should prioritize relationships with relevant platforms, have knowledge of pertinent laws and regulations, and be able to navigate various languages and time zones.

Fraudulent Advertisements and Unauthorized Account Pages on Social Media

Losses due to fraudulent advertisements are estimated to reach $100 billion annually by 2023. Rapid identification of these ads is critical to minimizing their impact, as the gap in time between abuse and removal can be costly.

Fraudulent advertisements on social media are created through both criminally-owned and compromised account pages on social platforms. Removal of an offending ad or page can be problematic, as brand abuse is not always obvious. Most platform authorities will require unmistakable evidence of fraud, and security teams should submit clear incidents of abuse.

Most of the top social media platforms have individual reporting features to communicate malicious activity on an ad or page. To pursue takedown, security teams should provide all information directly or indirectly related to suspicious activity. This includes fraudulent sponsored advertisements and links to any unauthorized content. When reporting abuse, security teams should submit as much evidence as possible to eliminate any doubt that infringement is occurring. Mitigation criteria includes:

- Logos
- Copyrighted material
- Trademarks
- Active links to sites hosting malicious content
- Look-alike domains
- Any available context around the offending ad or page

Fraudulent advertisements on social media are easy to create and modify and may be altered by threat actors to appear generic after abuse has been reported. To reveal past abuse, security teams should use platform security feeds to submit as proof of former misconduct.

It is particularly helpful to establish relationships with platform providers to expedite the removal of malicious activity.

Counterfeit Websites and Look-alike Domains

Counterfeit websites often use malicious domains to appear legitimate. These domains can be hosted by a variety of providers, each with its own unique policies for takedown. Some providers may be non-compliant, in which case security teams should escalate takedown requests to an upstream host or authority.

Security teams should establish strategic relationships with a variety of providers, including:

- Registrars
- Hosting Providers
- Network System Providers (NSPs)
- Internet Service Providers (ISPs)
- Computer Emergency Response Teams (CERTs)

Registrars will require clear documentation proving abuse of Intellectual property or a trademark, including look-alike domains, source code, and logos. To increase the odds of successful takedown, proof of related abuse should also be provided, including URLs or infrastructures hosting malicious content.

Conclusion

The collection and mitigation of counterfeit activity targeting businesses can be complex. Threat-types and definitions of infringement vary, and it is not always clear when a threat is associated with counterfeit activity.

To expedite the identification and removal of unauthorized activity, organizations should proactively prioritize relationships with platforms and providers, gather data through a combination of automated and human collection, and provide high-fidelity evidence that will prove abuse. Successfully mitigating online counterfeit threats can be time-consuming but is critical to protecting your brand and reputation.

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.