ZEROFOX

5 Step Guide to Brand Protection

Follow these five steps to bolster your brands and business against frauds, fakes, and cyber attackers outside the perimeter.

TABLE OF CONTENTS

Introduction

Your brand often serves as the face of your organization.

Before a customer or prospective employee interacts with your business, they've likely interacted with your brand online. In fact, of the 5 billion+ people online worldwide, **51.6% use the internet to research brands, products, and services before making a purchase (that's over 2.5 billion people!). Additionally, 43.6% of social media users are looking for information about brands and products.**[1] That's what cybercriminals are counting on.

Brand attacks and scams are on the rise. In the ZeroFox ecosystem, we've seen a 519% year-over-year increase in security incidents specifically related to online scams. These include:

- 295% increase in HR scams
- 609% increase in money flipping scams
- 100% increase in impersonating profiles

The impact of a brand attack can be massive, from financial losses to tarnishing your brand's established reputation. In fact, in a recent survey, 40% of respondents said they disengage with a brand's community after only one exposure to a toxic impersonation, with 45% saying they lose all trust in a brand after an impersonation or attack.[2] This goes beyond a simple PR problem.

Organizations must protect their investments in social and digital platforms by detecting, identifying, and remediating brand abuse incidents outside the perimeter on the surface, Deep, and Dark Web. **That's where brand protection comes in.**

Brand protection is the cybersecurity practice of monitoring digital channels and platforms to detect and remediate brand abuse and impersonation threats. The goal is to effectively safeguard the brand's reputation and protect its employees, customers, and online community.

An effective brand protection strategy allows organizations to preserve their digital reputation while putting an end to fraudulent content, impersonations, account takeovers, trademark infringements, and other forms of malicious brand abuse. Let's take a look at the 5 most important and simple steps to create a mature brand protection strategy.

1 Hootsuite Digital 2022 July Global Statshot Report

2 https://www.businesswire.com/news/home/20210629005298/en/Survey-Nearly-Half-of-Americans-Quickly-Lose-Trust-in-a-Brand-If-Exposed-to-Toxic-or-Fake-User-Generated-Content-on-Its-Channels

5 Steps to Improved Brand Protection

With this understanding of why protecting your brands beyond the perimeter is vital to your cybersecurity posture, it's time to outline the necessary tactics that comprise an effective brand protection strategy. Start with these five steps.

ZEROFOX

Step 1:

Conduct an Audit and Define Your Needs

Your brand likely operates across a variety of digital platforms and channels. You may also manage a portfolio of brands with a myriad of connected assets across these channels. You'll need to address which elements you own and where they're hosted – and subsequently at risk – online.

Start with an audit of all of your branded assets that exist in the "gray space" (sites and spaces where you, customers, and threat actors actively engage on the internet that none of you own). You'll need to create a repository of all of your logos, brand terms, sub-brands, domains, etc. You'll also want to consider any high-profile executives, employees, or VIPs to monitor.

Next, take inventory of your attack surface. This requires assessing the various digital channels and data sources where your brand has a footprint.

Your digital footprint isn't limited to corporate social media accounts and owned domains. Consider any digital channel where customers or employees engage with your brand or branded assets. For example, although your business might not have a dedicated and moderated Reddit forum, customers may be susceptible to impersonations and scams that exist on the platform. Likewise, illicit sites and Deep and Dark Web channels may pose brand risks such as intellectual property (IP) piracy, counterfeiting, leaks, and infringement.

Once you have a list of all of your protected assets and a bird's-eye view of the external attack surface, you can more easily identify gaps. Using this view, map your biggest risks and identify potential challenges with your security team. These might include identifying sites you may have little access or visibility to, or where to reallocate team members to manage your presence on these sites.

Typical Use Case

Acme Ltd. owns several affiliated brands, including BurnBright Sparkles, BurnBelly Hot Sauce, BurnCalories Carrot Cutters, and BurnBoredom Craft Glue. These brands all have individual logos and elements on dedicated social media pages like Facebook, Instagram, LinkedIn, Pinterest, and TikTok. They also each have help forums and branded content across various review sites.

ZEROFOX

Step 2:

Establish Proactive Protection Measures

Once you've audited your brand's assets and mapped out your attack surface, you can take a few proactive protection measures. To start, make sure you've registered all trademarks and domains and have defined valuable assets as well as use cases.

If you're using an external threat protection platform, you'll also need to properly configure threat alert rules and parameters. For example, you'll want to set up alert rules that cut through the noise and trigger only when your security team needs to know or take action. It's critical to minimize false positives and hone in on the threats that pose an immediate security risk.

It doesn't stop there. You'll also need to proactively register domains with common typos.

You'll do the same for social media. Proactive domain registration and social media account creation with common misspellings, variations, and homoglyphs prevents hackers from targeting your brand or executives through "typosquatting" impersonations.

Additionally, there's a misconception that having no social media presence means you're without risk on those channels. In reality, it's quite the contrary — you may be facing increased impersonations on platforms where you don't typically operate or frequently monitor. For that reason, it's a best practice to create profiles and accounts on all social media channels for your brands and high profile executives.

Typical Use Case

A dancewear company, Tiny Dancer LTD, has registered their domain TinyDancer[.]com. They also have decided to proactively register domains with common typos, like tinnydancar[.]com, tineydancer[.]com, tonydanza[.]com, etc. which redirect to the correct domain. They'd also register for social media profiles with the same misspellings.

ZEROFOX

Step 3:

Leverage Continuous Brand Monitoring and Automation

Protecting your company outside the perimeter requires 27/7 digital brand protection; it is ideal for security teams addressing external threats to their brand, executives, data, and customers.

Monitoring for malicious domains, fake accounts, attack chatter, and account takeover attempts is an effective way to ensure the only people engaging with your followers and customers are legitimate.

However, the sheer number of brand impersonations online make them difficult to tackle manually.

In a report published in May 2020, ZeroFox observed almost twice the number of malicious domains compared to 2019 figures. In the first half of 2022 alone, ZeroFox observed over 2.7K malicious domains on behalf of customers with over 7.5K unique malicious domains from July 2021-July 2022. Without relying on some sort of automation, it would be nearly impossible to detect these brand impersonations at scale, particularly if they aren't using a direct name match.

Impersonation detection automation often used in digital risk protection software monitors for risky behavior on key accounts. This includes detection of account takeover attempts and brand abuse, like trademark infringement, logo misuse, piracy, and leaked proprietary content. Through your software, you'll establish and tune automation rules to watch parked domains and domain registrations for similar keywords through the collection of multiple data sources across the web. This requires a combination of AI analysis and detection of metadata, logos, reverse image searches, and text.

Furthermore, you'll need the ability to dive deeper than the surface web to process and analyze information across the Deep and Dark Web. Dark Web forums, which you may otherwise be unable to access, house the Underground Economy where your information and protected assets could be up for sale. Automated monitoring via scraping of these forums can help you uncover attack chatter or sensitive data leaks and breaches that mention brand assets such as IP, product names, and domains.

Typical Use Case

Ace has several threat actors targeting them across a variety of channels. Using automation and continuous monitoring, the company found that an online scammer was spoofing their social media profile on Facebook and offering fraudulent discount codes in exchange for personal info from followers (names, DOB, etc). Further, the Ace security team found sensitive customer user information for sale on a hacker forum from a recent data breach through Dark Web monitoring.

ZEROFOX

Step 4:

Employ Human Analysis and Intelligence

Due to the sheer volume of raw threat data you need to ingest and analyze, it can be difficult to discern what poses an immediate threat. AI models with technology such as computer vision can help reduce the noise and add context, but you still need the critical component of human intelligence for impactful brand intelligence.

Brand intelligence, which is a function of cyber intelligence, specifically focuses on protecting an enterprise's digital presence.

Brand intelligence solutions employ humans to collect and analyze data across public and digital platforms, including surface, Deep and Dark Web, social media, mobile app stores, and more with the unique focus on identifying risks to the organization's brand(s), products, and data.

Typically, a human SOC analyst team will analyze the data collected by automated methods. They'll review alerts, triage threat levels, and either escalate them to the correct party or provide a deeper level of investigation. Through this process, you'll gain clarity that just isn't possible with automation alone.

Human intelligence will also monitor Dark Web forums and chat rooms for brand mentions that can help you thwart attacks in the planning phase or quickly identify potential threats or breaches. For example, they'll help you decipher early warning signs of attacks wherein personal identifying information (PII) has been leaked, etc.

Human intelligence is also critical for providing contextual recommendations for actioning, such as applying risk scoring for detected threats or facilitating content takedowns.

Human intelligence is especially important when physical security is involved. For example, if there are threats made online targeting your physical location, you'll need help to efficiently and effectively identify the credibility of threats to inform your response.

Typical Use Case

SodaCo has more than 100 brands globally, with multiple branded assets (such as domains, social accounts, etc.) set up for each brand in each country where they operate. On Instagram, SodaCo's threat detection automation alerted on an imposter storefront using the name ChipCo, one of SodaCo's protected brands. Human analysts then worked with the SodaCo brand, corporate communications, and legal teams to act on the alert in an effort to take the impersonating profile down. This ultimately stopped the store that was claiming false affiliation with those brands.

ZEROFOX

Step 5:

Implement Adversary Disruption for Threat Remediation

Threat remediation activity has grown significantly. Across all industries, **ZeroFox has seen a 94% year-over-year (YoY) increase in scam takedowns submitted and then subsequently removed.**

You must pursue various takedown types to disrupt the adversary who is creating the malicious content and scams. These include the takedowns of impersonating social accounts, infringing domains, IP abuse, piracy, etc. Each of these takedowns may require differing steps, such as working with providers, proffering evidence, and following specific processes for removal per that provider's takedown request policies.

Taking on this process manually can be time-consuming and expensive. Instead, many organizations choose to either leverage specialized takedown services or rely on services provided by their cybersecurity vendors.

For example, removing offending content from social media is a much different process than removing a fraudulent website in accordance with the domain host or registrar. It's a good best practice to establish and maintain provider-specific runbooks that capture the takedown types, policies, and processes needed to effectively prosecute takedowns for each use case. If you decide to work with a managed service provider, it's important to choose a vendor that specializes in all takedown types.

In addition to takedowns, remediation of brand threats can also come in other forms. For example, remediation may include the addition of known malicious domains to industry block lists (like Google Safe Browsing). When a bad actor attempts an account takeover, remediation may also include the triggering of other automated actions like locking down branded social accounts. Typically, a managed service provider can execute these actions.

Typical Use Case

Piper Strickland Paper Company has detected an impersonator on social media who posts malicious content and directs followers to a fraudulent site with fake coupons. To disrupt the bad actor, Piper Strickland works with a managed takedown service team that specializes in removing malicious domains and fraudulent accounts. The takedown team works directly with the network providers on behalf of Piper Strickland to provide evidence of the Terms of Service violations and works within the parameters set by the network providers to have the content successfully removed. Additionally, the managed service team submits indicators of attack extracted from the takedown request to various third-party partners (such as ISPs, hosts and registrars, industry block lists, etc.) to block access to malicious content and disrupt future attacker campaigns.

Find and Eliminate Brand Attacks with ZeroFox

The most effective way to improve your brand protection is to implement a security vendor that is purpose built to identify and remove impersonating accounts, domains, scams and other malicious content.

ZeroFox's brand protection software secures your organization against account takeover, fake accounts, spoofed domains, and scams targeting customers, in which attackers exploit brand logos, messaging and product photos to defraud customers. ZeroFox comes pre-packaged with rules and policies targeting the identification of these impersonation attempts. With over 800,000 takedowns processed annually, ZeroFox has the ability to scan over 23 million URLs weekly, and has a strong network and relationship with hosts and registrars, ISPs, social media networks, and other web providers to disrupt the adversary.

ZeroFox provides best-in-class centralized & automated protection of owned brand channels and assets with brand threat intelligence use cases.[3]

Digital Brand Protection from ZeroFox enables companies to:

- **Protect brand investment**
- **Maximize customer engagement**
- **Focus on promotion**

3 The Forrester Wave™: External Threat Intelligence Services, Q1 2021

About ZeroFox

ZeroFox, a leader in external cybersecurity, provides enterprises external threat intelligence and protection to disrupt threats to brands, people, assets and data across the public attack surface in one platform. With global coverage across the surface, deep and dark web and an artificial intelligence-based analysis engine, the ZeroFox Platform identifies and remediates targeted phishing attacks, credential compromise, data exfiltration, brand hijacking, executive and location threats and more. The patented ZeroFox Platform technology processes and protects millions of posts, messages and accounts daily across the social and digital landscape, spanning LinkedIn, Facebook, Slack, Instagram, Pastebin, YouTube, mobile app stores, domains, cloud-based email and more. ZeroFox and the ZeroFox logo are trademarks or registered trademarks of ZeroFox, Inc. and/or its affiliates in the U.S. and other countries. Third-party trademarks mentioned are the property of their respective owners.

Ready to step up your brand protection?

Ready to step up your brand protection?
Let's get started.

Visit zerofox.com to learn more.