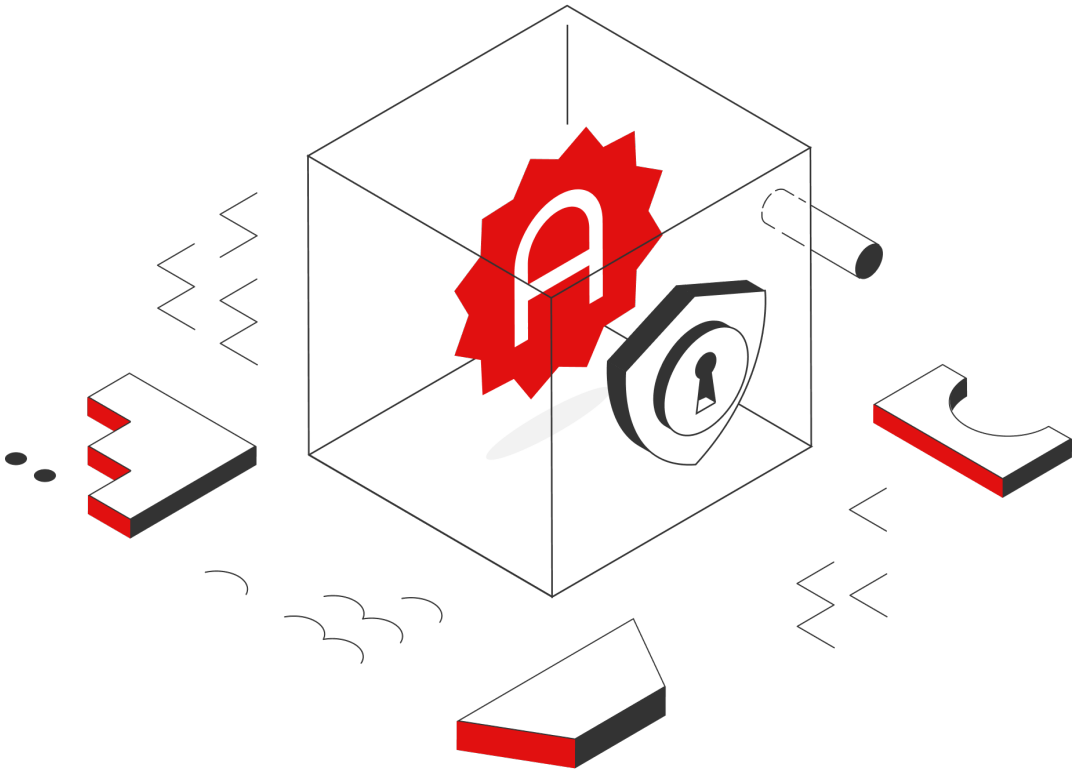


RED SIFT

eBook

WHY MODERN BRAND PROTECTION STARTS WITH SECURING YOUR DOMAIN

Contents

BOOK YOUR FREE RED SIFT PLATFORM DEMO TODAY

Introduction

A company's brand isn't just a logo, trademark, or rulebook. It's the identity that solidifies its values, distinguishes it from competitors, and ultimately underpins its purpose. A strong brand takes time and effort to cultivate, and it is intrinsic to a business' success. In fact, 46% of consumers will pay more for brands they trust.[1] It's no wonder that brand protection is creeping up the priority lists of global businesses in 2022.

There was a time when the term brand protection signified tightening trademarks, cracking down on counterfeits, and retrieving intellectual property. But with businesses today experiencing rapid digitization, near-reliance on the internet, and adoption of new technologies, the surface area for attack is vast, and sadly brand abuse has branched out. Online brand abuse, particularly that which relies on domain impersonation and fraud to be successful, is more achievable than ever, making effective brand protection increasingly complex.

In this eBook we explore modern brand protection, how it thrives in today's digital landscape, and why an effective brand protection strategy aimed at preventing fraud starts with securing your domain.

1 . A brief history of brand protection

What is brand protection?

In its simplest form, brand protection refers to the strategy, tools, and rules a business has in place to prevent bad actors from abusing its brand. By implementing a brand protection strategy, you're not only safeguarding your reputation and revenue, you're also protecting anyone that comes into contact with it - including your customers.

What is modern brand protection?

The Cambridge English Dictionary defines brand protection as;

> *The act of preventing someone from illegally making and selling a product using a brand name owned by another company.*[2]
>
> CAMBRIDGE ENGLISH DICTIONARY

Modern brand protection isn't solely centered on preventing the sale of counterfeit physical goods. Rather, it's about stopping attackers from achieving their goals by disabling their ability to use digital and online methods to do so, as well as monitoring brand assets to ensure legitimate use. This isn't to say that counterfeiting and intellectual property theft aren't still significant issues. But as attackers' methods for achieving these goals (among others) have evolved to become entrenched online, methods for preventing this must as well.

Unlike more traditional brand protection methods which employ specific staff and professionals to monitor and tackle brand abuse, modern brand protection primarily uses brand protection technology, software, and automation.

What is brand abuse?

Brand abuse comes in all shapes, sizes, and forms, but ultimately the term is used to describe the infringement of a company's brand by an outside party or attacker. This party will use your business' reputation for its own gain, at the expense of your brand equity.

85% of businesses experienced a brand infringement in 2019[3]

Traditional methods of brand abuse include:

- Counterfeiting and Counterfeit Products
- Trademark Squatting
- Copyright Piracy
- Intellectual Property Theft

Modern methods of brand abuse include:

- Fake or 'Lookalike' Websites
- Online Logo/Asset Misuse
- Business Email Compromise
- Exact Domain Impersonation (Spoofing)
- Email Impersonation
- Scam Campaigns and Phishing Attacks
- Fake Social Media Accounts
- Malicious Mobile Apps

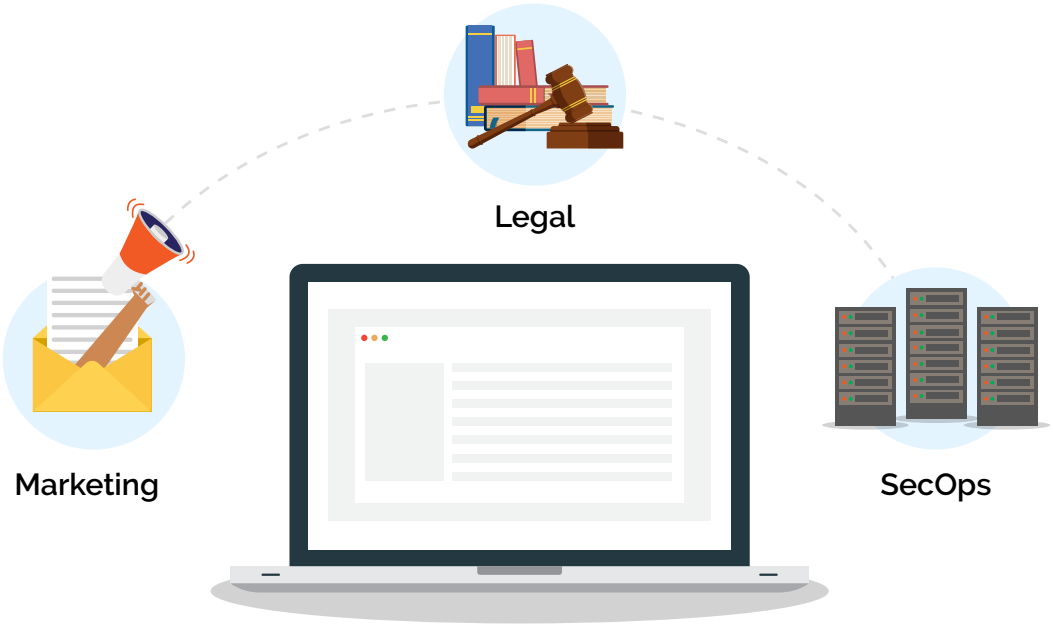
While the traditional methods of brand abuse are still rife, it's clear that the advent of online has enabled a whole new playing field for bad actors to play on. Businesses need to be empowered to protect their brand both online and offline, and from all angles.

> *One of the greatest inventions of my time is certainly the World Wide Web and the prosperity it has brought to many nations and people globally. It is this same prosperity in electronic communication that has permitted the growth of nefarious activities aimed at generating benefits for some at the expense of harm to all others.*[4]

David S. Howard
OUTREACH SPECIALIST
BRAND PROTECTION 2020: PERSPECTIVES ON THE ISSUES SHAPING THE GLOBAL RISK AND RESPONSE TO PRODUCT COUNTERFEITING

2. "That's not my domain!" Whose problem is brand protection?

Traditionally, the responsibility for ensuring a company's brand protection has sat with legal and brand professionals. However, there are a number of departments in organizations that need to take a vested interest in brand protection in 2022.



Marketing

Since marketers are responsible for building a company's brand in the first place, and any harm to its reputation will impact the business long-term, they should be taking a keen interest in how it is protected.

Legal

A company's legal team will want to ensure that brand infringement, fraud, and abuse are prevented through monitoring and enforcement, both by dedicated professionals but also relevant brand protection technologies that harness automation.

Security Operations (SecOps) & Information Security

Many cyberattacks now start with brand impersonation, fake websites, and other forms of brand abuse relating to security infrastructure and company domains. So, security operations and information security professionals need to be poised to prevent this.

77% of brands say brand safety is a key priority[5]

3. Why brand abuse thrives in a digital landscape

Today's world is overwhelmingly digital, and brands worldwide utilize ecommerce and online channels every second to operate and grow. The shift to ecommerce that we've seen in recent years holds a host of benefits for businesses, including vastly improved customer reach, increased capacity for sales, better customer experience, and improved automation.

Ecommerce sales are expected to hit $7.3bn by 2025[6]

But with these benefits comes a downside: the bigger digital footprint a business has, the larger the surface area for attack - and brand abuse - becomes.

> *It merely takes a computer, some easily accessible enabling tools such as a domain registry, search-engine optimizer, payment providers, shippers, and a worldwide storefront to establish a business.[7]*

Leah Evert-Burks
DIRECTOR OF BRAND PROTECTION
BRAND PROTECTION 2020: PERSPECTIVES ON THE ISSUES SHAPING THE GLOBAL RISK AND RESPONSE TO PRODUCT COUNTERFEITING

> *Many factors contribute to this (counterfeiting) growth, but none as significant as the growth of the Internet and the acceptance of online purchasing by consumers. That acceptance, combined with the financial rewards and minimal risks to the counterfeiters selling online, creates the "Perfect Storm" for continued rapid expansion.[8]*

Ron Davis
SENIOR DIRECTOR OF BRAND PROTECTION
BRAND PROTECTION 2020: PERSPECTIVES ON THE ISSUES SHAPING THE GLOBAL RISK AND RESPONSE TO PRODUCT COUNTERFEITING

4. Modern brand protection starts with securing your domain

In this online landscape, your domain is synonymous with your brand identity. It's your shopfront, your way of representing your brand online, communicating with and selling to customers, and ultimately growing your business. It's no surprise then, that bad actors make every effort to exploit it, piggybacking off the hard work you've put into building it, using it to commit fraud, and damaging it for the long term.

5-10 years

The average time it takes for bigger corporations to build up and establish a successful brand.[9]

So, when it comes to protecting your brand online, you need to start by securing your domain. Unless you're protecting this, people can start trading off your hard work, and using your brand to commit fraud.

Brand protection is value preservation

Every business wants to generate value, but what about preserving it? Effective brand protection - protecting the brand you've built, keeping control of what you've already created, and safeguarding the investment you've made in it - is in itself an important form of value preservation.

> *Experienced gladiators when entering the Colosseum in ancient Rome intuitively understood that their chances of victory and survival were enhanced if they were in possession of both a sword (offense) and a shield (defense). Similarly, a prudent board in the 21st century should also intuitively understand that their chances of successfully and sustainably navigating the corporate minefield is enhanced if they are in possession of both value creation and value preservation capabilities. This is simply logical and basic common sense.*[10]

Sean Lyons

VALUE PRESERVATION & CORPORATE DEFENSE AUTHOR, PIONEER, AND THOUGHT LEADER

5. What measures should you take to secure your domain and prevent the brand abuse that leads to fraud?

Logo and asset detection and management

Organizations risk irrevocable reputational damage when phishing attacks are successful using their counterfeit logos. Not only is revenue and market share at risk, but trust too; victims of these attacks will remember the brand associated with the phishing scam, even if the brand itself was also a victim of the phish. A logo detection service determines that assets are being illegitimately used, and these findings then increase the speed with which a takedown can be initiated.

71% of UK consumers say they will stop purchasing from a company altogether if their trust is broken.[11]

BIMI with VMC, enabling use of legitimate logo in email

Brand Indicators for Message Identification (BIMI) is a standard that displays validated trademarked logos for all DMARC-authenticated emails. As email continues to be the most popular way organizations communicate, BIMI adds brand impressions to every email to help reassure recipients that it is from the organization it claims to be from. In research carried out in partnership with Entrust, we found that the use of BIMI increased consumer confidence in the legitimacy of an email by 90%.[12]

29.5% of 2,380 domains owned by the largest publicly traded companies in the largest economies in the world are BIMI-ready.[13]

Lookalike domain investigation, discovery, and takedown functionality

Much of the success of today's online brand abuse hangs on the attacker's ability to spin up a lookalike website domain. Having sent out their phishing email (or other form of attack), they can then direct their victim to a fake site, harvesting credentials, money, and more. This is a very common tactic, with research showing that a new phishing website goes live every 20 seconds.[14]

To combat this, it's crucial that businesses include lookalike discovery and takedown functionality as part of their modern brand protection strategy. By using functionality that ensures parked, forgotten, and impersonation domains are uncovered and removed, you can actively block attackers attempting to use your domain (and brand) to commit fraud.

Every 20 Seconds a new phishing website is published and goes live.[15]

Implement DMARC at p=reject

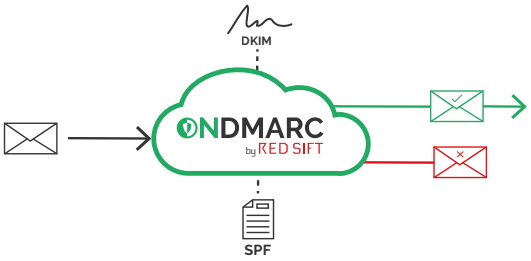
Over 333 billion emails are sent every day,[16] and this is still a channel widely used by businesses for everything from operations to communications and offers. So it's no surprise that it's a key vector that bad actors continuously use for attack.

Implementing DMARC at its strongest policy of p=reject is the first step to securing your domain against brand abuse. By doing this you are blocking bad actors from impersonating your domain to carry out phishing attacks, Business Email Compromise, and other types of fraud via email, and stopping them from tarnishing your brand. DMARC is the foundational layer of protection for your most valuable and vulnerable digital asset: your domain.

Phishing accounts for **90% of all data breaches**.[17]

Impersonation attacks were named the second most disruptive to a business by the UK Government Cyber Security Breaches Survey in 2021.[18]

What is DMARC?



DMARC (Domain-based Message Authentication, Reporting, and Conformance) is an outbound email security protocol that - when implemented at the strongest policy of p=reject - protects domains against exact impersonation i.e. when a bad actor impersonates an organization's domain to send phishing emails to its employees, customers, and supply chain. It works using existing protocols SPF and DKIM.

2.1% of 64 million apex domains researched had DMARC at enforcement, meaning 97.9% are at risk of exact domain impersonation attacks.[19]

Secure your inbound email with advanced threat detection and response

Secure Email Gateways (SEGs) and phishing awareness training alone don't work. To complement these, a layered email security approach that augments traditional training with 'in the moment' communications should be adopted. This will help drive down BEC and impersonation attacks from unprotected businesses, and help prevent attackers infiltrating your business and brand.

39% of participants failed to spot a phishing email when they didn't have the help of Red Sift's OnINBOX advanced threat detection banners and indicators.[20]

The best brand protection strategy is a layered one

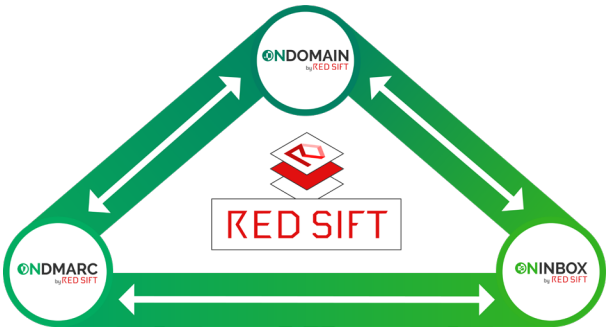
While the above measures are essential building blocks for protecting your domain perimeter and in-and-outbound email against modern brand abuse and fraud, there's no silver bullet, and your brand protection strategy should be a layered one. Other brand protection best practices to implement include market surveillance, commercial insights, distributor compliance, incident management, customer and staff awareness programs and training, among others.[21]

6. How Red Sift's Platform helps stop cybercriminals using your brand to commit fraud

It's clear that in today's day and age, brand protection and prevention of brand abuse to commit fraud need to be addressed from every angle, not least by securing your domain, as well as your in-and-outbound email infrastructure.

At Red Sift, we enable security-first organizations to successfully communicate with and ensure the trust of their employees, vendors, and customers. Our Integrated Email Security and Brand Protection Platform is made up of a number of gold-standard and award-winning products: OnDMARC, OnDOMAIN, and OnINBOX. These are designed to work in unison to block outbound phishing attacks, analyze the security of inbound emails, and provide domain impersonation defense for company-wide threat protection.

1. **OnDMARC** blocks the most sensitive attack vector: the impersonation of real domains
2. **OnDOMAIN** uncovers and disarms impersonation domains as they are being prepared and before they can reach the inboxes of customers, counterparties, or the wider public
3. **OnINBOX** detects and flags inbound email threats for users, providing protection at the point of interaction



Find out how the Red Sift Platform can help your business mitigate modern brand abuse such as lookalike domains, domain impersonation, BEC & logo abuse

BOOK YOUR FREE RED SIFT PLATFORM DEMO TODAY

RED SIFT

About Red Sift

Red Sift enables security-first organizations to successfully communicate with and ensure the trust of their employees, vendors, and customers. As the only integrated cloud email and brand protection platform, Red Sift automates BIMI and DMARC processes, makes it easy to identify and stop business email compromise, and secures domains from impersonation to prevent attacks.

Founded in 2015, Red Sift is a global organization with international offices in the UK, Spain, Australia, and North America. It boasts a client base of all sizes and across all industries, including Domino's, Telefonica, Pipedrive, Rentokil, Wise, and top global law firms. Find out how Red Sift is delivering actionable cybersecurity insights to its global customers at redsift.com.

References

1. Salsify (2022); Consumer Research Report - The value of building brand trust
2. Cambridge English Dictionary
3. Marketing Week (2020); Brand safety, trademark infringement, marketing budgets: 5 killer stats to start your week
4. David S. Howard, Center for Anti-Counterfeiting and Product Protection, Michigan State University (2020); Brand Protection 2020: Perspectives on the Issues Shaping the Global Risk and Response to Product Counterfeiting
5. IAB Europe, Marketing Week (2020); Brand safety, trademark infringement, marketing budgets: 5 killer stats to start your week
6. Statista (2022); Retail e-commerce sales worldwide from 2014 to 2025
7. Leah Evert-Burks, Center for Anti-Counterfeiting and Product Protection, Michigan State University (2020); Brand Protection 2020: Perspectives on the Issues Shaping the Global Risk and Response to Product Counterfeiting
8. Ron Davis, Center for Anti-Counterfeiting and Product Protection, Michigan State University (2020); Brand Protection 2020: Perspectives on the Issues Shaping the Global Risk and Response to Product Counterfeiting
9. Security Boulevard (2021); Definitive Guide to Modern Brand Protection
10. Sean Lyons (2021); Value Preservation Increasingly Acknowledged as Primary Purpose and Fiduciary Duty
11. Adobe (2021); 7 in 10 Customers Will Buy More from Brands They Trust; Abandon Those They Don't
12. Red Sift (2021); Consumer Interaction with Visual Brands in Email
13. Red Sift (2022); BIMI Radar
14. JAMF (2021); Market Guide for Mobile Threat Defense
15. JAMF (2021); Market Guide for Mobile Threat Defense
16. Statista (2022); Number of sent and received e-mails per day worldwide from 2017 to 2025
17. Cisco Umbrella (2021); Cybersecurity threat trends: phishing, crypto top the list
18. Department for Digital, Culture, Media & Sport (2021); Cyber Security Breaches Survey 2021
19. Red Sift (2022); BIMI Radar
20. Red Sift (2021); Breaking the chain: can email banners and indicators change the behavior that leads to breaches?
21. Mark Monitor (2016); 12 Best Practices for a Successful Brand Protection Program