Whitepaper

mimecast®

How to help prevent increasingly rampant brand exploitation

A trio of brand protection activities can reliably protect your brand from cyber spoofing

Brands have been the unwitting victims of scams since time immemorial. Now, in the age of phishing, it's worse than ever. Sophisticated brand exploitation lures have been used to kick off some of the world's most devastating cyberattacks. Many organizations think they're helpless to do anything about it. But with a combination of DMARC records, AI-based advanced brand protection systems, threat intelligence sharing and improved user awareness, brand owners can effectively combat even the most nefarious fraudsters.

Key Challenges

- Brand exploitation attacks have two camps of victims: the brand itself and the brand's customers/recipients. Consequences are diverse and can be wide-reaching.
- Organizations rely on a number of digital channels to engage with stakeholders, multiplying the opportunities for cyber criminals to deploy exploit attacks.
- No brand is safe. Bad actors target organizations of all types and sizes.
- Differentiating legitimate from illegitimate emails can be a challenging, as many organizations authorize third parties to send emails on their behalf, such as through customer relationship management (CRM) systems.
- Brands commonly overlook the need to proactively hunt for threat actors beyond the perimeter, meaning they have no idea when they're being impersonated and for what purpose.
- Humans are, simultaneously, the weakest link in protecting against brand exploitation and an indispensable line of defense.

Overview

Malevolent actors are highly adept at exploiting brand names and likenesses to create scams that prey on human nature, vulnerabilities, and trust. These threat actors trick innocent victims into trusting impersonated emails, websites, mobile apps, and social media posts, usually to harvest credentials, drop malware, or conduct fraud. The consequences are costly: For one, people who fall for brand exploit attacks put their personal information—and often their organizations—at risk by opening the doors to harmful data breaches or broad-based infections. Meanwhile, every time a brand is exploited, its reputation and value are threatened.

What's more, brands may never know they're being maliciously impersonated unless they go out and look for it—a challenge in itself, since cybersecurity controls commonly

Recommended solutions:

- To protect themselves and all stakeholders from brand exploit attacks, brands need a multi-layered, proactive cybersecurity approach. The best defense is a good offense.
- Domain-based Message Authentication Reporting and Conformance (DMARC), an email authentication standard introduced in 2012, can help brands identify unauthorized email senders and help ensure that only valid emails reach recipients.
- Advanced brand protection systems using AI and machine learning are emerging; they actively hunt and can shut down spoofed domains and websites, helping to prevent brand exploit attacks before they are executed.
- A strong and cautious user base can be a strong last line of defense. Regular cybersecurity awareness training fortifies the human firewall, helping individuals detect brand exploit attacks to safeguard themselves and their employers.
- Consuming and sharing threat intelligence is a key way to discover malicious attacker infrastructure.
- By stopping brand exploit attacks before they happen, companies can reduce the amount of harmful cyberattacks—benefitting the internet community as a whole.

consist of network monitoring and perimeter defenses as opposed to proactively hunting threat actors across the web. But anti-brand-exploitation strategies must be robust enough to protect both brands and customer/recipient victims, while encompassing every potential consequence.

Perimeter-based email security controls alone won't cut it, cyber awareness training alone won't cut it, and brand protection systems alone won't cut it. But DMARC email authentication, advanced brand protection systems, threat intelligence sharing, and strong user awareness and caution can significantly reduce the risk of brand exploiting attacks.

What is brand exploitation?

It's astonishingly easy for bad actors to impersonate brands to dupe customer/recipient victims, which is why an equally astonishing 81% of IT and IT security decision makers, in research by Mimecast and Vanson Bourne, experienced web or email spoofing attacks in the past year—averaging nine attacks each.[1] The simple fact is that it's easy to take advantage of human nature. Whether it's through a compromised email account or lookalike web domain, social media or an app, sneakily exploiting a company's digital presence helps bad actors prey on the established relationships between a brand and its stakeholders.

Moreover, the same research shows 74% said they anticipate their company's volume of web spoofing, email spoofing, and brand exploitation attacks will increase over the coming year. Without the right brand exploitation prevention strategy, brands and individuals will each continue to fall victim to brand abuse. Brands often have no idea their likeness and name are being exploited, and attacks can be so clever that individuals usually don't know they've compromised themselves—and their companies—until it's way too late.

Understanding how brand exploitation attacks work

To understand why a such a comprehensive online brand protection strategy is needed to combat brand exploitation, it's important to take a close look at exactly how bad actors carry out their attacks—and how complicated the consequences can be for both the exploited brand and the individual customer/recipient victims who take the bait.

Prepping the lure

First, the attacker identifies their target victims: the brand to be exploited and the recipients of the attack. Bad actors can strike at any time for any reason, but they often take advantage of trends and current events to prey on human nature, desires, anxieties, and uncertainties. This was highly evident during the COVID-19 outbreak in early 2020, which saw a 30.3% increase in impersonation attacks,[2] and a subsequent 80% leap in unsafe clicks in companies that don't use cybersecurity awareness training.[3]

With COVID-19 as the impetus, bad actors took advantage of human desire for information during a time of uncertainty by mimicking authoritative sources of global health information, such as the CDC and WHO. They preyed on financial worries by spoofing emails promising fake government payouts. Global travel bans were used to send links for fake airline ticket refunds. And a desire for leisure in spite of stay-at-home orders led to a massive spike in domains impersonating popular streaming services, offering "free" subscriptions with the goal of harvesting victims' credentials.

But a brand exploitation attack can happen any time. A simple fraudulent email from the local coffee shop with a link promising an employee a free birthday latte can wreak havoc just as swiftly as a hacker masquerading as a financial services company during an economic crisis.

Casting the bait

Next, malicious actors choose their delivery mechanism. Usually they spoof a brand's email domain or register a copycat website by cloning the HTML from the legitimate website—right down to a brand's recognizable color scheme and logo. This is distressingly easy for several reasons:

- Anyone can pretend to be somebody else in the "from" field of an email, and there's no internet police to stop them. DMARC records identify exact copy domain frauds, but it can't prevent an attacker from sending an email from a lookalike domain.
- No one can stop a bad actor from registering a domain that looks just like a legitimate brand's domain name. All it takes is a subtle difference in characters, such as an intentional typo user are likely to make, or even exploiting the international domain system to register domains with non-English characters that look like English ones.
- Even the least tech-savvy bad actors can purchase cyberattack kits. In simplest terms, attack kits are a dark form of software-as-a-service that typically let bad actors add malware-deploying lures to spoofed domains.

Reeling it in

Whatever the lure, cyber criminals tend to use spoofing techniques that put pressure on the attack recipient. For example, they might lure an unsuspecting individual with an urgent email claiming a fraudulent purchase was made with their credit card. The email may have a link to a just-as-realistic-looking login webpage, but it's designed to drop malware or steal their credentials. And if the recipient clicks the link, they open the door—and their organization's door—to whatever the criminal's heart desires. Meanwhile, the credit card company may have to deal with reputation damage or other consequences.

Brand exploitation attacks can be that simple, but they're often layered. Criminals commonly use spoofing techniques to phish for credentials. Since people frequently use the same username and password across multiple accounts, they may then be able to access the victim's finances, personal email, work email, and more. This can lead to internal account-takeover phishing campaigns within an organization, malware deployment, data breaches or ransomware attacks - all stemming from one email impersonating a well-known brand.

High stakes and complicated consequences

So it is that even the most basic brand exploitation attacks can open up a can of worms. It's no wonder the average total cost of a data breach is $3.92 million.[4] And all it can take is the combination of one brand who has no idea its likeness is being exploited, and just one unsuspecting victim who clicks an unsafe link.

One, Two, Three, (Four) Punch!

- **DMARC**
- **AI-based advanced brand protection systems**
- **Extensive Treat Intelligence sharing**
- **Security awareness training**

Solutions

With such a wide attack vector, online brand protection solutions must be broad and deep. But traditional perimeter security approaches aren't enough, since damage is usually being done entirely outside your perimeter.

Importantly, though, new capabilities have emerged in recent years to help meet the brand exploitation challenge. Specifically, the one-two-three (four) punch of:

1. DMARC
2. AI-based advanced brand protection systems
3. Extensive Treat Intelligence sharing
4. Security awareness training

With a brand protection strategy combining all three, brands can take back the reins and better control how they are presented everywhere on the web, protecting not only themselves but their customers as well as other potential recipient victims.

1. DMARC cannot be overlooked

The world as we know it couldn't exist without email, and no brand-customer communication platform has a wider reach. But email's inherent flaw is that trust is implicitly assumed across users, so that if a brand has no rigorous email authentication strategy anyone can send illegitimate emails that claim to come from that brand's domain. Brands need a tool that makes certain that every email sent to their customers, employees, or anyone else, is authentic.

Enter Domain Message Authentication Reporting and Conformance, better known as DMARC.

What is DMARC?

Officially published by the Internet Engineering Task Force (IETF) in 2015, DMARC is an email authentication and reporting protocol that enables brands to do two key things:

- Collect information on who is using their domains and how. This includes phishers and legitimate third parties working on behalf of the brand.
- Tell recipient email servers which emails are genuine and how to deal with unauthenticated emails.

DMARC builds on the prior SPF and DKIM email security standards, which, in a nutshell, are discrete email authentication mechanisms added to a domain's DNS record to help prevent email spoofing. While effective, cybercriminals have devised ways to bypass SPF and DKIM. DMARC links SPF and DKIM, taking outbound email security a step further by letting domain owners—such as brands—publish customizable policies in their DNS record that helps email servers detect (and even reject) phony emails before they can reach a victim's inbox. The more brands that use DMARC, the more protected a brand's outbound email is, and the more every single email user is protected from spoofed emails.

Still, the Mimecast and Vanson Bourne research found that only 28% of respondents were using DMARC, and only 22% of that group had deployed a "reject" policy—DMARC's highest level of enforcement. Getting to full DMARC enforcement can be tricky, which likely contributes to that low adoption rate to date. But it's worth it. And this is why the usage of DMARC continues to grow.

How DMARC works

Every time an email is sent from a domain with a DMARC record in place, an inbound mail server checks the message to determine if:

- The message comes from an IP address permitted by the domain's SPF records
- The DKIM signature is valid
- The message's "from" header aligns with the sending domain

Using DMARC, brands can instruct an inbound mail server what to do with messages that fail this check: nothing (other than report), quarantine in spam folder, or reject.

DMARC provides two comprehensive reports to brand owners: aggregate reports, which provide an overview of all email traffic, including IP addresses that have tried to exploit domain names; and forensic reports, which send similar info in near real-time whenever an email fails the DMARC check.

DMARC for brand email discovery

Because of the way it works—and those reports—DMARC can be used not only for enforcement but, critically, for "discovery," too. As the key first step toward incrementally building a full-fledged brand protection program, brands can use DMARC in a discovery phase to identify all the email being sent on its behalf—legitimate or not. Daily aggregate and forensic reports are key here. It can be exhausting for larger organizations with many domains, CRM service providers, and third-party marketers or other legitimate email channel users to pore over long reports. But it's a necessary step to build the brand's knowledgebase and avoid inadvertently blacklisting authentic emails. Third party DMARC solutions are available to help organizations fast track their DMARC journey.

Once a brand has confidence that it has completely whitelisted legitimate email and rejects attempted forgeries, it can set its policy to have receivers reject the delivery of illegitimate messages—the gold standard of DMARC enforcement. Now, brands can protect their own reputations and prevent innocent recipients—and their organizations—from becoming victims of brand exploitation attacks. Unfortunately, DMARC itself can be a challenge to configure and use. So much so, in fact, that Gartner says third party tools are a virtual necessity for analyzing and acting on the large amount of data it generates.

> ***"Using a third-party tool or service to manage and implement DMARC is often the most effective way of getting to the point where emails can be rejected if they fail DMARC,"*** March 2020 Gartner report.

Still, when properly implemented, DMARC can be highly effective at causing the rejection of illegitimate emails. But it can't prevent emails sent from lookalike domains.

2. Big data, bigger defense: The power of advanced brand protection solutions

While brands and their customers enjoy the endless possibilities of modern digital networks, cyber criminals take advantage of the same technological advancements to continuously devise new cyberattack schemes. They take advantage of a brand's lack of visibility beyond its perimeter by swiftly registering spoofed web domains—and other key digital touchpoints—that resemble legitimate sources.

It's not uncommon for criminals to leverage automation to put up and take down their own spoofed websites, creating a moving target. By the time a security team finds out about the impersonation, the source is gone ... until it reappears elsewhere. Every moment spent investigating a false trail or a non-incident means resources are diverted from finding legitimate attacks when they're in action.

Fortunately, new AI-based advanced brand protection solutions with massive web searching capabilities have the capacity to keep brand exploitation attacks at bay. And by protecting themselves, brands protect their customers and other potential victims, too.

What are advanced brand protection solutions?

Using specialized algorithms, advanced protection systems analyze endless troves of data and intelligence to identify sophisticated, fast-moving brand exploitation attacks—24/7/365.

There are three main functions advanced brand protection solutions perform to help brands protect themselves and their customers beyond their network perimeter.

Proactive hunting in the wild: Online brand protection solutions scan the entire world wide web for suspicious activity, all day and all night. They're capable of spotting spoofed domains, social media pages, mobile apps, and any other copycat attempt to exploit a brand for malicious purposes.

Brand domain monitoring: Through an embedded web agent, brand protection systems provide a kind of tireless vigilante always on the lookout for cyber criminals scraping a web site and deploying it on a foreign domain.

Automated takedown: Using APIs, advanced brand protection systems can be set to automatically notify internet registrars and hosting providers to takedown confirmed malicious impersonation web pages, usually within hours. This automation can be tied to a threshold level of suspicion—and can highly accelerate the elimination of threat, sometimes even before the attacker deploys.

Experts monitoring brands 24x7: While tools and automation are critical, expertise is also critical to discovering and taking down brand exploiting web sites. The most effective services combine monitoring with security operations expertise to help wade through suspicions and confirm what are actually real attacks.

Advanced brand protection solutions

Advanced brand protection solutions use AI, machine learning technology, threat intelligence and automation to perform two critically important functions.

They:

- Constantly monitor a brand's domains—and all other digital touchpoints—to detect potential bad actors scraping content for use in related spoofing attacks
- Actively hunt for malicious spoofing attempts throughout the wild, wild web

3. Fortifying the human firewall

No matter what a brand does to protect itself from impersonation, it's ultimately the strength and caution of the human firewall that determines whether a brand exploitation attack succeeds. But 94% of corporate data breaches involve human error.[6] Humans are clearly the weak link when it comes to protecting themselves and their organizations—but they can also become an indispensable line of defense.

The best way for individuals to protect themselves and their organizations against brand exploitation attacks is to develop the skills to detect even the most subtle attacks. Brands stand to benefit from teaching their employees to do just that. Even if a brand uses DMARC and advanced brand protection solutions to protect itself, that won't prevent its employees from falling victim to attacks that impersonate other brands.

Discerning the fake from the authentic requires a keen eye, but the human firewall can only be strong if employees engage in cybersecurity awareness training at regular intervals—ideally at least monthly —to keep up with the evolving threat landscape. And regular awareness training works. According to a Mimecast customer study during the coronavirus pandemic, employees at companies **without security awareness training were 5.2 times more likely** to click on dangerous links than employees that did receive regular awareness training.

Conclusion:

Any way a brand regularly communicates with its customers in the digital sphere becomes potential bait for a brand exploitation attack. If a bank's regular customer communications include emails suggesting they login to their online accounts, phishers can send similar emails to harvest a victim's credentials. Such attacks are constantly evolving to leverage new technology and take advantage of human vulnerabilities.

DMARC records are a vital step in preventing brand exploitation attacks, but not the only step. AI-based advanced brand protection solutions proactively hunt damaging brand impersonation attempts far beyond a brand's network perimeter. And a strong human firewall creates a powerful last line of defense, enabling employees to protect themselves and their organizations against risk.

Above all, the fight against brand exploitation does more than help brands protect themselves from experiencing the worst-case scenarios of cyberattacks. By stopping brand exploit attacks before they can happen, brands play a role in reducing the amount of cyberattacks that can potentially harm any email recipient and their organization—benefitting the entire global business community.

[1] State of Email Security Report, Mimecast | [2] Threat Intelligence Briefing: Surging Spam and Impersonation Attacks Drive Increasing Coronavirus Cyber Threats, Mimecast Blog | [3] Threat Intelligence Briefing: Security Awareness Training Helps Dramatically Reduces Unsafe Clicks Amid Surging Coronavirus Cyber Threats, Mimecast Blog | [4] Cost of a Data Breach Report 2019, IBM | [5] Protecting Against Business Email Compromise Phishing, Gartner Inc. | [6] 2019 Data Breach Investigations Report, Verizon | [7] Threat Intelligence Briefing: Security Awareness Training Helps Dramatically Reduces Unsafe Clicks Amid Surging Coronavirus Cyber Threats, Mimecast Blog