Solution Brief

mimecast

Tackling Phishing, Impersonation and Brand Exploits

Why a multi-layered approach using best-in-class tools is needed to protect your brand, your customers, and employees.

Staying one step ahead in a fast-moving threat landscape demands a proactive, multi-layered approach to cyber security. With phishing representing the number one attack vector, organizations should begin by protecting their own email system and the employees that trust and rely on it every day. But you can no longer stop there.

Attackers are increasingly using your online brand as bait, launching lookalike websites to trick your customers, partners and wider supply chain into divulging credentials, sensitive information and even handing over money. These attacks are often invisible and put your brand and reputation at risk.

The impact these attacks have on organizations and their customers is huge, with phishing making up a significant proportion of the $6 trillion in cybercrime costs. While household brands may be more valuable targets to impersonate for illegal gain, no business or organization is immune.

Read on to better understand the risk associated with this growing problem, the tactics being used, and how you can not only protect your organization and employees, but also your customers.

Deception works

Roughly **90% of data breaches** occur on account of phishing.[1]

30% of phishing messages are opened by recipients.[2]

Brand impersonation has **risen by more than 360%** since 2020.[3]

A new phishing site is created on the internet **every 20 seconds.** [4]

What's fueling the growth in brand attacks?

The global economy is increasingly digital. Organizations are embracing digital channels as a way to drive revenue growth, connect and engage with customers, and help their staff be more productive. This digitally-powered economy is fueling the advancement of brand exploits as attackers prey on the trust we have in the companies and organizations we deal with for banking, broadband, collaboration, social interaction, parcel delivery and more. The same holds true in a B2B context.

We expect and demand instant connection to the brands we use, accessing web content, and ordering and communication with them online. We receive promotional emails, social posts, and targeted online display ads. This digital reliance gives attackers an opportunity to hijack the brands we trust to improve the success of phishing emails and websites.

To make matters worse, the lines between our home and work lives have never been more blurred. We've found ourselves toggling between producing work documents and shopping for gifts online, creating the perfect storm for cybercriminals to deceive - with credential theft, data exfiltration, and financial gain all top of mind.

The risks of inaction or inadequate protection can be devastating

There are significant risks in not taking the appropriate defensive and offensive actions to protect your brand, reputation, customers, suppliers, and employees.

These include but are not limited to:

- Stolen company and customer data
- Financial loss (money transfer, revenue, and lost business)
- Brand and reputation damage
- Lost employee productivity
- Compliance fines (GDPR), legal fees, and clean-up costs

Defending against phishing, impersonation and brand exploits

To successfully tackle brand exploits and deception tactics, it's useful to look at the mechanics of how these attacks work, including the preparation and execution stages. There are essentially two targets; the employees and the customers of the organization whose brand is being exploited. Attackers can target either or both.

73% **of organizations have suffered a direct loss following an impersonation attack.[5]**

Successfully tackling brand exploits needs a multilayered approach. Breaking the problem down in terms of who is being targeted helps to understand the different methods needed to protect each one.

Let's focus on your employees first. Your employees are being targeted predominantly via email by sophisticated attackers posing as trusted senders. This can include impersonating other employees by spoofing your domain (both direct and lookalike domain spoofing) but also by spoofing trusted third parties like your suppliers and customers. In fact, 88% of organizations in a recent survey confirmed they had seen email-based spoofing of business partners or vendors.[6]

In addition to email, attackers are using other methods and tools to entice action; for example, malicious links in social media, personal email and instant messaging apps. Protection for these other potential attack vectors is a critical consideration.

Mimecast Web Security

Integrates with the Email Security service to extend protection to all the places employees click or browse.

Protect your employees with:

- Email security that includes protection against advanced spoofing, impersonation, and Business Email Compromise (BEC).
- Internal email protection to monitor and hunt down malicious content that may already be inside your perimeter.
- Data Leak Prevention (DLP) to help stop both malicious and accidental exfiltration of sensitive data.
- Web security that blocks access to malicious websites including those attempting to steal credentials.

88% **have seen spoofing of business partners or vendors.[6]**

How Mimecast can help

Comprehensive solutions are key

Mimecast Email Security with Targeted Threat Protection includes **Impersonation Protect** that is designed specifically to detect and stop spoofing attacks, whether they are impersonating your own or another trusted brand.

By identifying combinations of key indicators in an email to determine if the content is suspicious, Impersonation Protect delivers effective protection against targeted email attacks even in the absence of a malicious URL or attachment.

Impersonation Protect:

- Protects against newly observed and newly registered domains used as part of an attack.
- Protects against display name spoofing and reply-to address mismatches.
- Detects similar, or lookalike domains, including those using non-western character sets, and includes a Targeted Threat Dictionary managed by Mimecast to which custom terms can be added by your administrators.
- Ensures end users are protected at all times by blocking, quarantining or visibly marking suspicious emails.

Impersonation Protect works with Mimecast's URL and attachment protection capabilities for highly effective defense against email attacks that use weaponized attachments or malicious URLs.

Mimecast Email Security also includes **Data Leak Prevention (DLP)** functionality that can detect and prevent sensitive information being spread to external parties as well as internally. DLP provides a granular set of controls that can be used to detect and react to sensitive and confidential information contained in emails and their attachments, delivering real-time protection against leaks by email.

Monitor and hunt inside your perimeter

Internal Email Protect applies best-practice security inspections to internal and outbound email, which accounts for 60% of all email traffic. It allows you to monitor, detect, and remediate security threats that may already reside within your email systems. This type of protection is critical as a recent Mimecast survey found that 71% of companies had seen an attack spread internally. This could be caused by compromised or careless employees, or in some cases, those with malicious intent.

Internal Email Protect stops the spread of malware and sensitive information, internally and outbound, by inspecting mail for weaponized attachments, malicious URLs and violations of data loss prevention policies. Malicious content detected can be automatically or manually removed from mailboxes through the Mimecast dashboard or via API from your tool of choice. The service is always rechecking content against the latest intelligence to remove any newly identified malware.

When it comes to your customers, suppliers, and business partners, it can feel a bit like their security is out of your control. It's an uncomfortable pill to swallow knowing they could easily be duped by attackers using your brand (or some amalgamation of it) and, the fact of the matter is, many organizations are only as secure as their least protected business partner/customer.

In order to address this gap between securing your own environment and ensuring those you do business with are adequately protected from attackers using your brand, you need a DMARC enforcement and reporting solution to make sure the communications sent on your organization's behalf are legitimate, and an attacker hasn't managed to cut in and hijack the relationship.

Protect customers and your supply chain with DMARC (Domain-based Message Authentication, Reporting and Conformance)

Gain visibility of anyone using your domain without authorization, and ultimately block delivery of unauthenticated mail.

It's far too easy for cybercriminals to use your brand and domains to target customers, suppliers and others. Using DMARC to stop abuse of the domains you own is an effective defense against brand abuse and scams that can tarnish your reputation and lead to direct losses for your organization, your customers, and partners. Having an enforced DMARC policy enables an outbound layered protection against malicious actors sending email on behalf of an organization's domains. When a malicious actor sends an email attempting to spoof a domain, the receiver will reject messages that fail the DMARC check and never deliver those messages to the inbox.

Cybercriminals are determined and are constantly looking for new ways to successfully complete their mission.

They're automating attack techniques, registering domains that look like yours to exploit your brand to target those who trust it, and even cloning your website to steal credentials, personal information, and money.

Common targets include industries and organizations with large consumer bases, like retail, financial services and utilities, but many others including B2B companies are also at risk. The problem is that most organizations are blind to these stealth tactics. While gateway defenses can help protect your organization and employees, these tools are not able to protect your customers, partners, and others as their traffic does not flow through your gateway.

Organizations need to take a more proactive approach to this problem, one that can intelligently find live attacks but more importantly, identify potential threats before they become active and do damage. That means finding them at the preparation stage. And finding them is just the first step - you need to have the ability to immediately contain and block the threat.

How Mimecast can help

Discover attacks early. Take them down fast.

Mimecast DMARC Analyzer gives customers the ability to enforce DMARC policy at the gateway, and provides customers with DMARC visibility and reporting to make effective DMARC enforcement faster and simpler. **Mimecast DMARC Analyzer** is a cloud service designed to provide 360-degree visibility and governance across all email channels. It provides self-service email intelligence tools to reduce the time, effort and cost of implementing a DMARC policy and managing ongoing adherence.

Mimecast Brand Exploit Protect provides customers with the ability to take direct and immediate action on threats discovered outside of their perimeter to block potential and live attacks.

Using sophisticated machine learning techniques, the service runs quadrillions of targeted scans that identify even unknown attack patterns, blocking compromised assets before they become live attacks at the earliest possible preparation stages.

Mimecast Brand Exploit Protect:

- Protect employees, customers, partners and 3rd party vendors from phishing scams attempting to trick them by abusing domains that are similar to their legitimate branding.
- Identify and protect against attacks where cybercriminals have cloned a website for malicious activities against stakeholders.
- Block and take down both suspicious sites and active scams.

This approach is focused on stopping attacks at the earliest stages. It enables Mimecast customers to block any potentially malicious domains and URLs at the click of a button before they've had a chance to cause damage. This block extends across both email and web security for customers who use both Mimecast services. Brand Exploit Protect requires zero integration with your infrastructure and can start detecting potential and live attacks in minutes.

Mimecast Brand Exploit Protect

Allows customers to immediately block malicious or suspicious domains and URLs in the Mimecast system with a single click - for both email and web.

Proactively uncovers threats attempting to deceive and steal from your customers and wider supply chain.

1. PWG Phishing Activity Trends Report , 2019 I 2. CyberTalk I 3. Graphus I 4. Dataprot.net I 5&6. Mimecast Sate of Email Security Report, 2019