SOLUTION BRIEF

Tackling Phishing, Domain Impersonation and Cybersquatting

Reduce phishing risks and enhance email trust with DMARC Analyzer's protection framework.

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.

Defending against phishing and impersonation

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.

Protect customers and your supply chain

It's far too easy for cybercriminals to use your brand and domains to target customers, suppliers, and others.

Using DMARC to stop domain abuse is an effective defense against brand abuse and scams that can harm your reputation and cause losses to your organization, customers, and partners. Most organizations are blind to these stealth tactics. While email security protects your organization, it can't safeguard your customers and partners, as their traffic doesn't go through your security tools. Enforcing DMARC provides layered protection by blocking malicious emails from using your domains and never reach the user's inbox. DMARC verification checks give you visibility and control.

44% have seen an increase in misuse of their organization's brand via spoofed email.[6]

Deception works

- **Took the bait** within **10 minutes** of receiving a malicious email[1]
- **74% of all data breaches** involve people[2]
- **68.2%** domains contain no DMARC record[3]
- **A new** phishing site is created on the internet **every 11 seconds**[4]

Protect your employees

Your employees are being targeted predominantly via email by sophisticated attackers posing as trusted senders.

What makes people such an easy target for cyberattacks? In short, it's the tendency of humans to be just that – human. Our mistakes are often innocent and avoidable, caused by either a lack of knowledge, lack of attention, or lack of concern. But people aren't just the weakest link in the chain, they're also one of your organization's most valued assets. The need to protect our employees has never been greater. When employees are not equipped with the right tools – knowing what to look for or what to do when a threat arises – it's only a matter of time before a mistake is made.

DMARC noncompliance introduces risk

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 and customer loyalty
- Lost employee productivity
- Compliance fines (GDPR), legal fees, and clean-up costs

How Mimecast can help

Gain control of your domain

Mimecast's DMARC Analyzer solution protects your brand by providing the tools needed to stop spoofing and misuse of your owned domains. Designed to help you reduce the time required to become successfully DMARC compliant, the solution provides the reporting and analytics needed to gain full visibility of all your email channels.

Brand Spoofing Protection

- Get full visibility and governance of email - DMARC Analyzer provides the reporting and analytics needed to gain full visibility and governance across all email channels with reporting and monitoring alerts.
- Block targeted inbound attacks – Multiple domains or third parties sending emails on your behalf can be particularly challenging in achieving DMARC enforcement. DMARC Analyzer is designed to guide you towards a DMARC reject policy as quickly as possible.
- **Enforcement confidence - Get comprehensive support from our fully managed service, offering expert deployment assistance and ongoing guidance to help you maximize the benefits of DMARC Analyzer.**
- Rapid deployment and cost effectiveness - DMARC Analyzer's approach is unlike any other, providing a fast and simple DMARC deployment with intuitive self-service tools and integrated project management. Mimecast's DMARC Analyzer solution is delivered as a 100% SaaS-based offering for rapid deployment and cost effectiveness.

Mimecast Engage

Your security starts and ends with people; make them part of the solution with Mimecast Engage. Identify human-driven risk with unprecedented visibility, enabling you to take a smarter approach to training and deliver real security outcomes.

References:

1. CISA Phishing Infographic I 2. Verizon DBIR Report I 3. DMARC.org I 4. Dataprot.net I 5&6. Mimecast State of Email Security Report, 2023

Secure human risk with a unified platform.

Mimecast's connected human risk management platform prevents sophisticated threats that target human error. By gaining visibility into human risk across your collaboration landscapes you can protect your organization, safeguard critical data, and actively engage employees to reduce risk and enhance productivity.