Solution Brief

Tackling phishing and domain impersonation

Why a multi-layered approach 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, in fact they are the identities utilized in these types of attacks.

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

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]

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

Defending against phishing, impersonation, and cybersquatting

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.

Successfully tackling brand abuse 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.

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 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. The problem is that most organizations are blind to these stealth tactics. While email security can help protect your organization and employees, these tools are not able to protect your customers and partners as their traffic does not flow through your email security solution. Having an enforced DMARC policy enables 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. Gain visibility of anyone using your domain without authorization, and ultimately block delivery of unauthenticated mail.

Protect your employees

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.

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.

44%

have seen an increase in misuse of their organization's brand via spoofed email.[5]

Risks in not taking action

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 and resources required to become successfully DMARC compliant, the self-service solution provides the reporting and analytics needed to gain full visibility of all your email channels. Using DMARC to stop direct domain spoofing protects against brand abuse and scams that tarnish your reputation and cause direct losses for your organization, customers, and partners.

Brand spoofing protection

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 aggregated reporting, encrypted forensic reports, real-time reports, and monitoring alerts.

Block targeted inbound attacks
Multiple active and dormant domains or third parties allowed send emails on your behalf, can be particularly challenging in achieving DMARC enforcement. You can specify what to do when emails fail DMARC authentication checks thus changing your policy to P=Reject to protect your organization from inbound attacks. DMARC Analyzer's user-friendly service is designed to guide you towards a DMARC reject policy as quickly as possible.

Enforcement confidence
Get the help and assistance needed with built-in guidance, an extensive knowledge base, and flexible services including a fully managed service help manage DMARC deployment, mitigate risk, and safely block malicious emails without impacting transactional email channels.

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.

Detect and put an end to spoofing attacks

Mimecast Email Security Cloud Gateway (CG) includes impersonation protection that is designed specifically to detect and stop spoofing attacks, whether they are impersonating your own or another trusted brand. Mimecast Email Security protects employees all the way down to the point of risk, applying Social Graphing to map communications patterns, identify anomalies, and detect attacks that use techniques like file-less malware and social engineering.

Impersonation Protection

- Detects sophisticated, highly targeted email threats with social graphing technology, newly observed and newly registered or lookalike domains.
- Protects against display name spoofing and reply-to address mismatches.
- Ensures end users are always protected by blocking and quarantining suspicious emails.
- Engages users at the point of risk with warning banners embedded only in suspicious emails.

Mimecast Email Security also employs a combination of potentially misaddressed emails protection and Data Leak Prevention (DLP) functionality that can detect and prevent sensitive information being spread to external parties as well as internally.

Artificial Intelligence and Social Graphing, in conjunction with a granular set of controls which prevents possible instances of data loss caused by employees sending emails to the incorrect recipient or prevents sensitive and confidential information sent in emails and their attachments.

Internal Email Protect

Internal Email Protect applies best-practice security inspections to internal and outbound email, which accounts for most email traffic. It allows you to monitor, detect, and remediate security threats that may already reside within your email systems to keep attacks from spreading internally or to customers and partners. When Internal Email Protect detects unsafe, undesirable, or malicious content, you have the option to remediate this content from end-user mailboxes either automatically, or through the manual intervention of the administrator. This reduces the exposure time to malicious emails/content and identifies all instances of the malicious content to be removed from the mailbox(es).