HORNETSECURITY

DMARC MANAGER

THE SOLUTION TO EMAIL SPOOFING

Trust is the foundation of business email communications, but cybercriminals exploit this through email spoofing—impersonating trusted domains or individuals to commit fraud, often leading to Business Email Compromise (BEC) attacks.

THE IMPACT OF EMAIL SPOOFING:

» **Financial loss** from fraudulent emails (e.g., fake invoices).
» **Reputation damage** from impersonation, leading to loss of trust from clients and partners.
» **Increased risk of phishing attacks**, exposing sensitive company data.

DMARC: YOUR DEFENSE AGAINST EMAIL SPOOFING

DMARC (Domain-based Message Authentication, Reporting & Conformance) is a powerful email authentication protocol that helps businesses prevent email spoofing. It works alongside **SPF** and **DKIM** to ensure only authorized emails are sent from your domain, safeguarding your brand and communication channels.

HOW IT WORKS:

SPF checks the sending server's SPF record to verify that the email was sent from an authorized IP address. If the IP address is listed in the SPF record it passes the check, otherwise it fails.

DKIM checks if the email is cryptographically signed with the private key of the sending domain, then validates it against the correspon ding public key. A positive match results in a passed check, other wise it fails.

DMARC checks that the "From" address in the email is aligned to the same email domain that SPF and DKIM validated in their own checks.

Finally, the **policy tag** ("p") in the sending domains DMARC record tells the receiving server how to treat the email based the check results.

HORNETSECURITY

Setting up and maintaining DMARC, DKIM, and SPF policies can create configuration headaches, especially if you're managing this for large and complex organizations, managing many domains, multiple configurations, and potentially different requirements per domain.

BUT THERE'S A SOLUTION: **PREVENT DMARC CONFIGURATION HEADACHES WITH DMARC MANAGER**

WITH DMARC MANAGER YOU CAN:

- **Gain visibility** into who else is sending emails under a domain and return control to the domain owner, strengthening and securing brand reputation.
- Easily to set up and maintain **DMARC, DKIM** and **SPF** best practice-policies for multiple domains.
- Get insights into email delivery and authentication status, helping identify legitimate campaigns and potential spoofing attempts.
- Enhance email marketing strategies by ensuring that bulk emails are delivered by complying with authentication standards required by major email providers like Yahoo and Gmail.
- Strengthen your compliance with industry/global regulations such as PCI DSS, NIST, GDPR, HIPPA and more.

LEARN MORE

EMAIL: info@hornetsecurity.com | www.hornetsecurity.com