Improve Email Deliverability and Secure Business Reputation with Essential Tools

Email plays a vital role in finding and retaining customers. However, emails that fail to reach their targets represent critical missed opportunities. And when hackers successfully spoof company email addresses, your online reputation suffers. Addressing key components of email authentication helps you improve email deliverability and protect your business reputation.

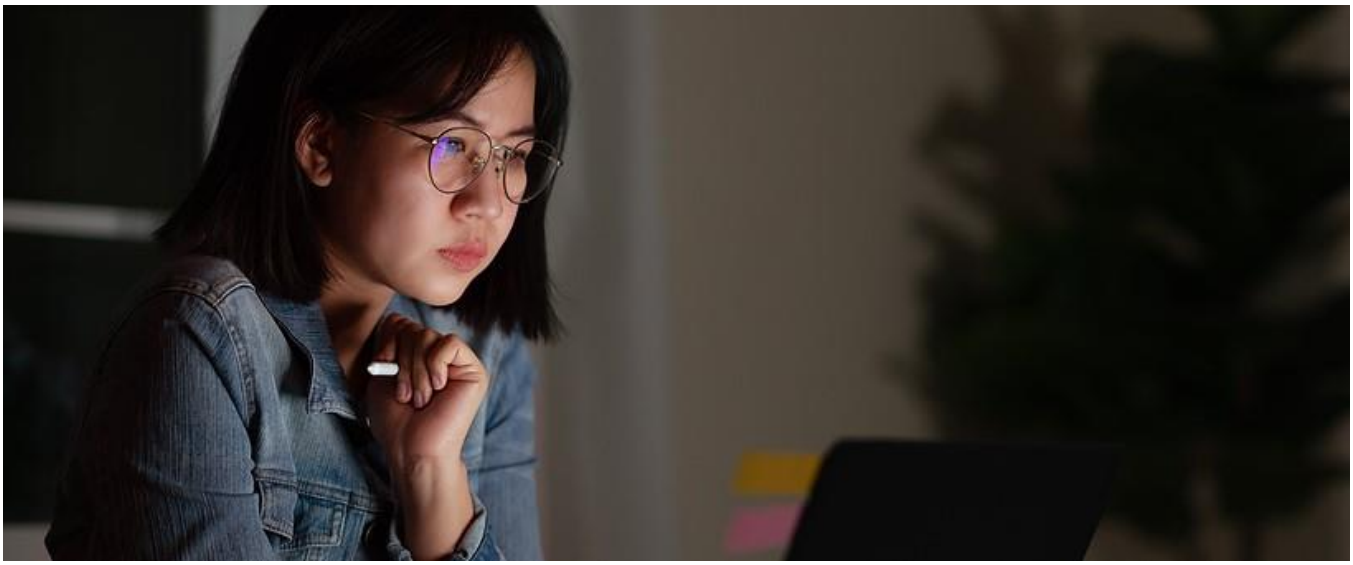
Emails can fail to reach their intended targets if the inbound mail server cannot verify the sender. For instance, in a spoofing attack, the hacker poses as a legitimate sender to trick the receiver into downloading malware or providing information. Consequently, if a receiving mail server doubts the authenticity of the sender, it may reject or quarantine an email.

Emails from your domain that get rejected by inbound mail servers can affect your business reputation. No business wants to end up on an email blacklist. Fortunately, the industry provides several tools to authenticate emails and guard against spoofing, spam, and phishing.

Terms to Know

As you set up your email framework for optimal use, you will need a basic understanding of the security tools available, including the following:

- SPF (Sender Policy Framework) – Your email administrator creates an SPF record specifying the IP addresses authorized to send email from your domain. The receiving mail server refers to the SPF record to authenticate the sender and determine whether to accept or reject the email.



- DKIM (DomainKeys Identified Mail) – DKIM provides a second form of email authentication using public key cryptography. The system attaches a digital signature to outgoing emails. Inbound mail systems then decrypt and verify the digital signature against a fresh version. This helps to ensure emails have not been modified or forged.

- DMARC (Domain-based Message Authentication, Reporting and Compliance) – DMARC uses SPF and DKIM protocols to provide visibility into email processing. Sending organizations create DMARC records specifying how to handle email that seems to come from their domain. This generally includes checking for SPF and DKIM compliance.

  The receiving mail server checks the DMARC record for instructions on how to handle incoming emails from a given domain. For instance, the DMARC may tell the receiver to reject emails that fail DKIM and SPF checks and to alert the sender about rejected emails.

Benefits of Implementing DMARC and Monitoring

Combining DMARC compliance with monitoring helps to preserve your company reputation while improving email deliverability. For instance, when you publish a DMARC record and correctly configure SPF and DKIM protocols, you prevent spoofing emails that appear to come from your domain. Even just publishing a DMARC record can improve your reputation.

Additionally, DMARC compliance increases the probability that inbound mail servers will accept your emails. In fact, some services will automatically reject emails that do not demonstrate DMARC or SPF compliance.

Pair DMARC with monitoring to keep on top of your email reputation. With properly implemented DMARC protocols, you will receive alerts to potential problems, including possible spoofing and blacklisting.

Experts Ensure Best Email Deliverability Possible

Implementing email protections to ensure deliverability requires careful system setup. Additionally, monitoring email reputation and making essential adjustments necessitates vigilance. eMazzanti offers the email protection services you need to provide peace of mind and protect your organization, including:

- Reviewing setup to confirm that approved senders appear in the SPF record. This ensures that email passes SPF checks to reach target inboxes.
- Preventing malicious spoofing by assisting with setup of DKIM service. This enables validation of your digital signature and verification of both SPF and DKIM authentication.
- Setting up DMARC for reporting about usage of your domain name. This provides insight into who is sending on behalf of your domain and how SPF and DKIM are being interpreted.
- Blacklist monitoring that adapts to how you send email from all your email senders, including third parties.

Protect your business-critical communication by partnering with the email deliverability experts at eMazzanti and their MXInspect Email Security products.