Set up SPF and DKIM for your Email Deliverability

One quick method to improve your email delivery rates is to incorporate SPF, or the Sender Policy Framework, and DKIM, domain keys identified mail, into your DNS settings. With this addition to your DNS entries, you're telling recipients that you've authorized Marketo to send emails on your behalf. Without this change, your email has a higher chance of being marked as spam since the email was addressed from your domain but was sent from an IP address with a Marketo domain.

You'll need your network administrator to make this change in your DNS record.

**SPF**

**If you DON'T have an SPF record on your domain**

Ask your network admin to add the following line to your DNS entries. Replace [domain] with the main domain of your website (ex. "company.com") and [corpIP] with the IP address of your corporate email server (ex. "255.255.255.255"). If you send emails from multiple domains through Marketo, you should add this to each domain (on one line).

```
[domain] IN TXT v=spf1 mx 4:[corpIP] include:mktomail.com ~all
```

If you need help setting up your SPF records, try the wizard on OpenSPF.org.

**If you DO have an SPF record on your domain**

If you already have an SPF record in your DNS entry, add the following to it:

```
include:mktomail.com
```
DKIM

What is DKIM? Why do I want to set up DKIM?

DKIM is an authentication protocol that is used by email receivers to determine if an email message was sent by who it says it was sent by. DKIM often improves deliverability of emails to the inbox since a receiver can be confident that the message is not a forgery.

How does DKIM work?

After you set up the public key in your DNS record (A), we will turn on DKIM for your outgoing messages, which will include an encrypted digital signature with each email we send out for you (B). The receivers will be able to decrypt the digital signature by looking up the "public key" in your sending domain's DNS (C). If the key in the email corresponds with the key in your DNS record, the receiving mail server will be more likely to accept the email Marketo sent on your behalf.
How do I set up DKIM?

To setup DKIM, place the following "public key" in your DNS record:

DNS Path:

M1._domainkey.[your domain].com

For example, Marketo's DNS path is: M1._domainkey.marketo.com

Public Key -- Download the attached text file (also listed below), copy the entire text, and paste as one line! The entry should be a single line, with a space between the semicolon and before the p. Due to the length of the public key, it may appear on multiple lines. Make sure your final entry has no line breaks:

```
k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDFUlNZvtGDIIGDRTzyRQydM9yRInD5YMx86QpgZ3v7pT+Mx4tGbJuxY41TXbsp7UH9hTREaKKGQQKNM/B3FzcFVv4zafZ09IUaXcbSdtD70iXyH0OXEGXLZl5gG0ZwjK5ptgQ18d+pUP9s8xMkJnZIubTk9MLvQnv3ZBzoL9FHDQIDAQAB
```

Open a Ticket with Marketo Support or Enablement

Once you've got the public key in your DNS, it's time to tell Marketo to "turn on" your DKIM signing. Please open a ticket with Marketo support or enablement. The Marketo Ops team will then schedule your DKIM activation and turn on signing at the scheduled time.

Note for Senders with Multiple From Address Domains

For senders that are using multiple From addresses that use different domains, you'll need to place a public key in each domain you want DKIM signed. Also, please make sure to include all the domains you want DKIM activated in your ticket with Marketo support or enablement.