Kibo Email Security Settings

To ensure email deliverability, Kibo recommends you implement SPF and DKIM email security protocols as part of your domain.

SPF

SPF is an email authentication protocol that helps prevent email spoofing and phishing attacks by verifying the sender's domain.

To add SPF validation, provide `spf.kibocommerce.com` in your SPF include.

For example, if you are sending emails from the domain "kiboclient.example.com", you should have an SPF TXT record that looks like the following:

`dig kiboclient.example.com txt`

```
kiboclient.example.com.       qq1600    IN    TXT    "v=spf1 include:spf.kibocommerce.com ~all"
```

DKIM

DKIM (DomainKeys Identified Mail) is another important email authentication protocol that helps prevent email spoofing by adding a digital signature to email messages.

You will need to add another TXT record. You can choose either "default", "kibodkim", or another selector of your choice.

```
TXT Record
default._domainkey.kiboclient.example.com
```

The values should be similar to this example:

```
"v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC7rHXysB4eCK7Lsn+7qRx
qQ0O9oNVvKtPxkWLMHL/TcXLR8jGtD42sYUBpd6O5dFOza5q1Dlb3z4U2HT9R+zwgcINloOiKZfordl2
0N+oVfLdBebv2Yyz/r+VY4QiP7HaNN4vkYCLCev/ynb/4EedzuLonWFRKEqVWug4E9qsDhQIDAQAB"
```

After adding this record, please submit a ticket specifying the selector you have chosen so that Kibo DevOps can add this record to the DKIM database.