verify your domain

email blaster

Email service providers (such as Microsoft and Google) use DKIM and SPF authentication to identify the legitimacy of your email. Without authentication, your email may arrive in the junk folder.

What do i need to do?

Verification is done by adding a SPF and DKIM record to your organisation's DNS server.

SPF: Create a TXT record for yoursite.co.uk with:

```
v=spf1 include:servers.ebsnd.com ?all
```

DKIM: Create a CNAME record for eb._domainkey with:

```
dkim.ebsnd.com.
```

NOTE: Replace “yoursite.co.uk" with the domain you want to authenticate.

If you are unsure how to do this, pass this documentation onto your IT department, or the person that manages your company website. Your domain registrar will also be able to provide assistance.

DNS changes can take up to 48 hours to fully propagate, however in most cases, propagation takes place within a few hours.

tips & tricks

A)

Depending on your provider, you may need to add quotation marks around your SPF record.

```
“v=spf1 include:servers.ebsnd.com ?all”
```

B)

If your domain already has a valid SPF record. Avoid creating a second record. Your existing and new record should be merged into one.

```
v=spf1 include:spf.protection.outlook.com include:servers.ebsnd.com ?all
```

C)

After adding your DNS record, allow up to 48 hours for the record to propagate (in most cases propagation takes only a few hours). After propagation, navigate to the sender profiles screen inside your email blaster, check that verification has been successful by clicking the refresh button on the verification screen next to your desired sender profile.