Osprey Approach: Allowing emails from Osprey on behalf of your firm

This help guide was last updated on
Jun 6th, 2023

The latest version is always online at
https://support.ospreyapproach.com/?p=837

Sometimes, you may have an issue with emails you have sent from Osprey bouncing back with a ‘rejected’ message or not being received at all. One example of this is password reset emails.

> Please note that only your domain hosts (the people who host your website) will be able to change the SPF records.

Because emails from Osprey will be coming from a different IP address than those sent from your mail server, some recipients may block these as spam or fake mail.

Your domain hosts need to add a record at the domain end to allow Osprey to send on behalf of this domain.

If your emails are with Office 365 the record should be added with the following format:

Type	TXT
TXT Name	@
TXT Value	v=spf1 ip4:94.228.39.160/27 ip4:80.253.115.96/27 include:spf.protection.outlook.com -all
TTL	1 Hour