Emails and SPF Records

A **SPF (Sender Policy Framework) record** is a type of Domain Name Service (DNS)**record** that identifies which mail servers are permitted to send an email on behalf of your domain. (TXT/SPF Record) protect from spammers or control how emails are handled. It also helps to prevent other people from using your domain to send spam or other malicious emails.

Recent updates in terms and conditions in Google, along with other email providers, have made SPF **(Sender Policy Framework)** Records even stricter to always look for SPF records for domains to ensure they are authorised to send email. Giving more and more difficulties to our customers in terms of their website functioning properly in communication and emails internally and with customers.

If your Sender Protection Framework (SPF) record does not include our servers, that means that your domain is set up to NOT allow us to send emails on your behalf.

In a given amount of time, the customer will receive one of the following possible scenarios related to their SPF Records:

- Error messages: "this sender failed our fraud detection and may to be who they appear to be".
- Outlook sending e-mails to "junk".
- User cannot send e-mails to certain domains.
- Customers are not getting the email confirmation of web orders.
- And other general issues with e-mail.

In case one of these cases appear the SPF Records need to be set or updated (to include us in them).

You can check your SPF records here: https://www.nslookup.io/

(When you check the domain on nslookup, please **add the URL without www at the beginning**).

--> Enter the e-mail domain (from the store e-mail address)

TXT records

SPF record

This record is valid for 1h.

Include the SPF record at spf.websell.io and **pass** if it matches the sender's IP.	include:spf.websell.io
Or else, **include** the SPF record at _spf.google.com and **pass** if it matches the sender's IP.	include:_spf.google.com
Or else, mark the email as softfail.	~all

In most cases, issues are caused by the SPF that doesn't have our IPs in it.

1) In case when we DO NOT control your nameservers, you will have to contact your host/email provider to include Websell in your SPF Records it has to include our record **v=spf1 include:spf.websell.io ~all.** It

does not matter if there are other domains included after **include:** provided that this is included so that the servers point to Websell servers.

NS records

Name server	Revalidate in
ns4.level3.net.	24h
ns3.level3.net.	24h

2) In case when we DO control your nameservers, please contact WebSell support, and we will update this record for you.

NS records

Name server	Revalidate in
ns1.nitrosell.com.	72h
ns2.nitrosell.com.	72h

Please note: changing '' -all'' to '' ~all'' is optional-- It makes other email servers a little more tolerant, but you can leave it at '' -all'' if you prefer