SPF, DKIM Setup Checklist

Sender Policy Framework (SPF) Setup

An SPF record consists of the following parts divided by spaces, where each part is processed in this order.

- **v=spf1** - version of protocol
- **mechanisms** - the ways to interpret allowed senders. Commonly used are: **a**, **mx**, **ip4**, **include**, **all**. At least one mechanism should be in the record:
  - **a**: All the A DNS records for domain are tested.
  - **mx**: All the A DNS records for all the MX records for domain are tested in order of MX priority.
  - **ip4**: A CIDR-spec is an IP network range. If no prefix-length is given, /32 is assumed.
  - **include**: The specified domain for the include is searched for a match. If the lookup does not return a match or an error, processing proceeds to the next directive. Warning: If this other domain does not have a *valid* SPF record, the result is a "Permanent Error".
  - **all**: This mechanism always matches. all should go at the end of your SPF record.
- Each mechanism has a **qualifier** - it represents the action which should be taken. The list of qualifiers:
  - **+** for a PASS result. It's used by default if no other qualifier is set, and is often omitted from SPF records.
  - **?** for a NEUTRAL result. No action should be taken (ignore that mechanism).
  - **~** (tilde) for SOFTFAIL. Mostly interpreted as "accept this message, but mark/tag it".
  - **-** (minus) for FAIL, the mail should be rejected.

Sample SPF records for domain xpass.com

The sample below shows an organization with domain xpass.com authorizing ue.hosted.com, IPv4:10.10.10.10 and spf.example.com to deliver emails in their behalf.

Record Type: TXT
Name: xpass.com
Value: "v=spf1 a:dispatch.ue.hosted.com ip4:10.10.10.10
include:spf.example.com -all"

Record Type: MX
Name: xpass.com
Value: ue1.hosted.com

IMPORTANT:
If you have an email security, marketing software, or helpdesk Salesforce, JIRA, Zendesk, or similar, they need to be authorized to send emails on behalf of your domain through your SPF TXT record.

Details are available on your respective platform's support site.

Mason Stevens Limited
ABN: 91 141 447 207 | AFSL: 351578
P: 1300 988 878 | E: info@masonstevens.com.au

Domain Keys Identified Mail (DKIM) Setup

When using DKIM, two problems of the email exchange are addressed:

- Verification of sender
- Assurance that content of the message was not altered during transit from sender's mail server to recipient's mail server

- DKIM records consists of the following attributes
  - v=DKIM1 – version protocol
  - k=rsa – algorithm used to generate the hash for the public/private key
  - t= - indicates the domain is testing DKIM or is enforcing a domain match in the signature header between the "i=" and "d=" tags
  - n= is a note field intended for administrators, not end users. The default value is empty and may contain a note that an administrator may want to read.
  - p= indicates the public key used by a mailbox provider to match to the DKIM signature.

For Office365 subscribers, please refer to the link
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/use-dkim-to-validate-outbound-email?view=o365-worldwide

Sample DKIM record for domain xpass.com

Record Type: TXT
Name: selector1._domainkey.xpass.com
Value: "v=DKIM1; k=rsa; n=core; t=s; p=MIIIPUBLICKEYSGOHERE"

IMPORTANT:

If you have an email security platform such as Symantec, ProofPoint, Mailguard, or similar, they need to be authorized to sign emails on behalf of your domain through a second DKIM TXT/CNAME record.

In addition, having your email security add a disclaimer will cause DKIM to fail because the body of your email has been altered in transit.

Verify your SPF and DKIM Records

Services you can use to test your domain SPF record:

- https://mxtoolbox.com/spf.aspx
- https://www.mail-tester.com/spf-dkim-check
- https://dmarcian.com/spf-survey/

Services you can use to test your domain DKIM record:

- https://mxtoolbox.com/dkim.aspx
- https://www.mail-tester.com/spf-dkim-check
- https://dkimcore.org/tools/dkimrecordcheck.html

Useful Links

- https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/how-office-365-uses-spf-to-prevent-spoofing?view=o365-worldwide
- https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/use-dkim-to-validate-outbound-email?view=o365-worldwide
- https://dmarcian.com/what-is-spf/
- https://dmarcian.com/what-is-dkim