How do I secure my e-mail delivery?

Every day, millions of e-mails are sent, of which many are abusive: spam, scam, phishing, ... How can you configure your e-mail in such a way, that the risk of e-mail abuse is minimized for your domain?

Below we quickly introduce you to DNSSEC, DMARC, SPF and DKIM. Let this information not overwhelm you: you can start gradually and even skip some parts. It will at least make your e-mail more secure than without any precautions!

0. DNSSEC

It all starts with DNSSEC. Simply because all of the e-mail security mechanisms described below rely on the DNS. With DNSSEC activated, no-one can mess with the DNS records and the e-mail security checks can be considered valid.

Enabling DNSSEC is very easy if you use the Openprovider nameservers: just enable it by updating your domain name.

If you use your own nameservers, or the nameservers of a third party, you will need to retrieve the DNSSEC key data and submit those to Openprovider by updating your domain name.

For more information about DNSSEC, you can read this article.

1. Enable reporting through DMARC

A good and very easy starting point is to enable reporting: using the DMARC protocol, receiving mailservers validate e-mails that are sent from your @domainname.com and send their findings to an e-mail address. There are many great tools available that process those reports and present them in a visually attractive and useful way. An example of such a tool is EasyDMARC.

All tools will guide you through the creation of the DMARC DNS record, so no knowledge is required yet. Just a simple TXT record in your domain's DNS record. Further down, we will come back to this.

The only important thing to take care of, is that the so-called *policy* in the DMARC record is set to *none*; your DMARC record should contain *p=none*. Using this value, your e-mail delivery will not be affected.

Once everything is set up completely, you will change this policy to make e-mail delivery more secure (see §5 below).

If you want to know more about DMARC, read our article about it.

2. Define who is allowed to send e-mails from your domain name with SPF

The next step is to define where your e-mail may come from. In other words: who is allowed to send e-mail from your @domainname.com. This is something that we cannot guide you through, but don't worry: you can start simple and keep tuning! It's done through the SPF (Sender Policy Framework) DNS record, and an example is the following:

```
domain.com.   IN   TXT   "v=spf1 a mx ~all"
```

The above record says that if the e-mail arrives from the IP address that's configured in the domain's A- or MX-records, it's trusted. Otherwise, let the receiving mailserver decide what to do.

The first task is to get an overview of what other servers you use to send your e-mails. That could include, for example, third party applications like mailing list or help desk software. Such application normally provides clear documentation about what should be added in an SPF record.

Read more about SPF records in this article.

You can generate, check and look up your SPF records using free online tools, such as this tool from EasyDMARC.

During the first weeks or months, you will (by the DMARC reports) find out if you omitted any sender, and tune your SPF record until it covers everything (see §5 below).

3. Sign (parts of) your e-mail with DKIM

Now that we have defined who is allowed to send e-mails from your @domainname.com, it's important to guarantee that the contents is not tampered with. This is done by signing parts of your e-mail in combination with the DKIM protocol. The receiving mail server will check if the signatures are correct.

DKIM must be configured on the mail server(s) that is/are used for sending e-mails. We cannot guide you through the settings of all such servers, but you can refer to our article about DKIM records for more information and hands-ons.

If you have difficulty enabling DKIM, remember that you can continue as well without it, you can always add it later!

4. Investigate DMARC reporting

Now all DNS records (SPF, DKIM or both) are set up correctly, it makes sense to check the DMARC reports. Remember: DMARC reports are gathered by the *receiving* mail server. Most DMARC tools will report the number of *compliant* and *non-compliant* e-mails.

Understanding report statuses

The *compliant* ones are the e-mails for which the receiving mail server could validate SPF and/or DKIM. Everything is in order, there's no need for you to analyse this further.

The *non-compliant* ones are most interesting: this report lists the e-mails that were sent from your @domainname.com domain, but did not pass the SPF and/or DKIM checks. For example, they were sent by a server that you forgot to include in your SPF record, or the signature check failed against the DKIM record, because someone forwarded the e-mail which caused the body to change.

And of course, it contains the e-mails that truly are worth reporting: the e-mail from the phishing sender, for example.

Improve configuration

Use this information to fine tune your SPF record and/or DKIM configuration. For example, add the IP address of the server you forgot to the SPF record, and change the DKIM settings so that no longer the full body is signed, but only the subject and the sender (for example).

Next time an e-mail is validated by a receiving mail server, such e-mail will be marked *compliant*.

Over time, you will discover that the number of non-compliant e-mails reduces, and in the end you'll see illegitimate e-mails only. All legitimate e-mails are marked compliant and you know your settings are correct.

Depending on the number of e-mails that you send, it might take up to many months before you are at this point.

5. Tightening SPF and DMARC policies

Now everything is in order, you can make validation stricter. This can be done in the SPF and the DMARC records:

- If you use the "softfail" qualifier in your SPF record (the tilde, ~), change it to the "fail" qualifier (the hyphen, -). This tells the receiving mail server to *explicitly reject* the e-mail if it does not pass the SPF check, instead of leaving this decision to the mail server.
- In the first step, we've set the DMARC policy to *p=none*, just to be sure it does not affect e-mail delivery. At this moment, all configuration is correct, so change the policy to *p=quarantine*. E-mails that fail the validations will then be put in the spam folder instead of the inbox. At a later moment, it's wise to change this to the ultimate policy *p=reject*: failed validations will not be accepted at all.

It's good to know that each receiving mail server may or may not follow the policies that you configured. It might be that a mail server accepts an e-mail, even while the SPF, DKIM or DMARC check fails! That is out of your control. Luckily, the majority of e-mails will be validated correctly.

6. Keep your configuration up to date

From now on, it's important to keep disciplined in updating your configuration. You won't be the first one that adds a server or changes his mailing list provider, and find that your e-mails are not delivered anymore because you forgot to update your SPF record.

With every change in infrastructure and applications, consider the potential impact on e-mail delivery and make the necessary updates.

The DMARC reporting remains a great tool to catch such issues: if you suddenly see a lot of e-mails being reported, that should be legitimate, it's time to change your settings!

Revision #2
Created 2026-08-07 14:31:57 UTC by Sarath
Updated 2026-08-07 15:48:48 UTC by Sarath