How do I add a DKIM record?

Email accounts · https://computancy.co.uk/kb/how-do-i-add-a-dkim-record/

DKIM, like SPF, is a standard that enables a specific aspect of the email sending process to be authenticated. The premise of DKIM is to check that an email is really from the domain or sender that it said it was sent from and if it has been altered in any way in transit.

Specifically, DKIM (DomainKeys Identified Mail), provides a foundation for distinguishing legitimate mail. A DKIM signature is placed in the header of emails sent by computancy's mail servers so that the receiving mail server can then validate the signature using a public cryptographic key (2048 bit). It's added as a TXT record in the Manage DNS section for the domain name.

DKIM does not outright mean all emails will be delivered. However, it does provide the receiving mail server with further information so it can make a more informed decision on the best way to handle the email.

To add one at computancy:

- Head to **Manage Hosting** and 'Manage' the package you want to add a DKIM record.
- Select the **DomainKeys** icon.

Firstly, we'll explain **how to add a simple DKIM record** to your DNS.

- Ensure you've selected the domain you want to add the DKIM record-to.
- Add a **Selector.** This can be any value or name you like. It's simply a field to identify the DKIM record. Then select **Add Signature**.
- If your nameservers are with computancy, we'll automatically add the correct TXT record for you.
- The signature will be added immediately to emails sent from the mailboxes under the domain selected. We will have automatically added a DNS record to **Manage DNS.** You may wish to wait for this to resolve for DKIM to be effective.

  From here you're all done: your emails will use DKIM as a method to authenticate email.

  You can also use the **Advanced Options** section.

Selector – This is a unique identifier for the DKIM record and can be set to any value you like. For example, you could set it to indicate the name of an office location or the signing date (e.g. “october2019”).

Granularity/Identity – By default, this is set to a wildcard value: '*'. You can use this field to set the DKIM record to be assigned to a specific mailbox, allowing you to constrain which mailbox can use this selector legitimately. For example, if you set the value of this field to be ‘sales’, only your sales@domain.com mailbox will use this DKIM signature. This field must match the local part of the signing address (mailbox).

Note – This field does not form part of the DKIM record or signature and is simply there so you can record any information about this record for your own information.

Service Type – Currently, DKIM only supports signatures added to messages sent via ‘Email’ (i.e. SMTP). However, in the future, the DKIM standard may add more service types such as IM or VoIP, which we’ll then be able to support. This field can be left to either ‘*’ or ‘Email’ - changing this won’t influence behaviour at present.

Canonicalization – Some mail servers and relay systems may modify an email in transit, potentially invalidating a DKIM signature. There are two options you can set: 'Simple' and 'Relaxed'. If you expect your email to be modified in any way, you should select **Relaxed** which is more forgiving to changes made the header and body of the email.

Expiry Time – This is the time which, when elapsed, the DKIM signature will be invalidated in the mail header. By default, it’s set to 86400 seconds (1 day). You may wish to extend this if you believe deliverability of the email will take longer than 1 day.

Flags - There are two flags available: 'Production' and 'Testing'. If you select **Testing**, you'll still receive a response to the email and the DKIM signature from the remote mail server, but the email won't be treated with different behaviour. Verifier systems may wish to track testing mode results to assist the signer. You'll mostly want to use **Production**.