DomainKeys Identified Mail (DKIM)

salesnexus

www.salesnexus.com

Chat with Us Here!

What is DKIM?

DomainKeys Identified Mail (DKIM) allows senders to associate a domain name with an email message, thus vouching for its authenticity.

In other words, DKIM is a protocol through which you can give authorization/permission to another service or platform to send out emails using your email address, on your behalf.

This is done by “signing” the email with a digital signature, a field that is added to the message’s header. A “signature” is generated by the sending mail transfer agent (MTA – the mail server) using an algorithm, applied to the content of the signed fields, which creates a unique string of characters, a “hash value.” When the signature is generated, the public key used to generate it is stored at the listed domain (your domain). After receiving the email, the recipient MTA (mail server) can verify the DKIM signature by recovering the signer’s public key through DNS. It then uses that key to decrypt the hash value in the email’s header and simultaneously recalculate the hash value for the mail message it received. If these two match, then the email has not been altered. This gives users some security knowing that the email did actually originate from the listed domain, and that it has not been modified since it was sent.

What’s its purpose?

In today’s digital age, there are many incidents involving email fraud or spoofing, where other people can imitate or spoof your email address and send out emails with fraudulent or malicious intents on your behalf without your knowledge or permission.

It serves as your digital email signature, telling the recipient’s email server that the email genuinely came from you as the sender, and not from other parties that are trying to use/forge your email address. Thus, this is an added extra layer of security and authenticity.

What's the effect of using a platform/service to send out emails on behalf of my email address(es) without DKIM?

Spam filters can detect emails that they receive, that does not have the digital signing (DKIM) or have not come from your actual email server, which increases the chance that the unverified emails (without DKIM), will reach the recipient's spam folder, or could be blocked by a firewall or network level spam filer or not even reach the recipient's inbox or spam folder at all.

Some, if not most of the email host/provider's anti-spam software, will treat email messages, that came from a different service/platform compared to where they claimed they were sent from, as dangerous, suspicious or a potential fraudulent email and will most likely tag them as spam or may even block them.

What does having DKIM with SalesNexus, have as an advantage for me?

Once SalesNexus and your email server provider/host setup a DKIM together, this will digitally "sign" all emails coming out from your SalesNexus account, as authorized/verified for us to send out emails to your recipients, using your email address on your behalf and with your permission. This will make spam filters see that the messages are being sent with your permission to recipients and will mark it as safe and legit.

Will having a DKIM setup with SalesNexus, guarantee a XX% deliverability rate?

There are a lot of other factors and elements to consider when it comes to email deliverability. We can't guarantee you a XX% deliverability rate with a DKIM setup, but you will notice that your deliverability rate will dramatically increase compared to not having one.

How do I request for DKIM setup?

Please let a SalesNexus customer service representative know that you're interested to have DKIM setup, to contact them, you can drop by in chat or email **support@salesnexus.com** and they'll be more than happy to provide you more details and guide you through the setup process.

DKIM Setup Process

Step 1

Upon receipt of your request for DKIM setup, your request will be processed and a "DKIM Key" will be generated. Your DKIM Key will be provided to you by our support team.

Step 2

Log into your domain host/registrar to set the key in the DNS Zone.

Example:

default._domainkey IN TXT "k=rsa;

p=MIGfMA0GCSqGSIb3DQEBAQU111BGNADCBiQKBgQC/zitpmnZnK5hs1v2o
gfa11BPfJpQYz6l+cjjEkQt84YesUtZmEMVDPa/T7oaliIi2JBHcO0TRtRF7FHNonu-
audXRMZlpbh2zXYWuamLDIVsltTak4FcH1SS+keWf81Q+irO7MSxBd5djTI8QCe+5
JH8ru9L9cgIFpx4h3Syd3cwIDAQAB"

The above is an example of the entry for the ISC bind zone file.

If you are using a web interface to set it up, you will need to set up a new TXT record with the following in one single line of text:

- The name set to: default._domainkey
- The value set in between the " " above.

Chat with Us Here!

Target, Connect, Convert

Step 3: Processing Complaints

To be able to continue to process complaints from @yahoo after setting this up, you need to forward abuse@***yourdomain.com*** to the **abuse@salesnexus.com** address. and you need temporary access to postmaster@*yourdomain.com* in order to register for the yahoo feedback loop here: **https://help.yahoo.com/kb/SLN3438.html**

Once the above setup is done on your end, kindly inform us as our technician can verify on our end if the key on our end and on your end, coordinate with each other.

*****Since this is an optional add-on, please inquire for possible applicable one-time fee for this setup.**