

A Step-by-Step Guide to Implementing DKIM for Safer Emails

Introduction

According to [Forbes](#), more than 300 billion emails are sent daily, of which 90% of spam and malware and just one click on any of these emails can lead to data breaches and ransomware attacks. To avoid these clients and email services, filter out emails, and your emails can likely end up in spam or trash folders. This can be avoided if you set up your SPF, DKIM and DMARC.

What is DKIM?

DKIM (Domain Keys Identified Mail) is an email authentication method which allows the receiver to verify that the authorized domain's owner sent an email and that the message has not been altered in transit. A digital signature is added to the message, which is encrypted and usually not visible to the end-users as validation occurs on the server-side. DKIM supports multiple digital signature algorithms such as RSA-SHA256, which helps in secure email communication, and prevents spam and spoofing of emails.

Why should DKIM be configured? (Risk)

DKIM helps overall mail authenticity and adds an extra level of security when configured properly with SPF and DMARC. If DKIM is not added, messages sent from your organization or domain will likely be marked as spam by receiving mail servers. Adding DKIM seems more legitimate to recipients and is less likely to end up in the Junk or Spam folders. Spoofing email from trusted domains is a common technique for malicious spam and phishing campaigns, and DKIM makes spoofing email from domains difficult. Over time, DKIM also helps in domain reputation and improves message deliverability.

How do DKIM records work?

DKIM works by adding a digital signature to email message headers. This signature is compared to the public cryptographic key stored in the business's Domain Name System (DNS) records.

In the domain's DNS record, domain owners publish a cryptographic public key as a TXT record. When an email is sent from an outgoing mail server, it includes a DKIM signature header with two cryptographic hashes for the header and body message. When the message is received, the inbound mail server examines its DNS for the sender's public DKIM key. This key first decrypts the signature before comparing it to a freshly calculated version. The message can be validated if they match.

How to add DKIM records in Google Workspace?

1. Sign in to your Google Workspace Admin console, then go to Apps -> Google Workspace -> Gmail -> Authenticate email address.
2. Click the Generate new record button after selecting your domain from the drop-down list.
3. Copy the generated text.

You must now create an accompanying record to associate that key with your email domain:

1. Log in to the admin console of your domain provider.
2. Locate the advanced DNS configuration page.
3. Generate a new TXT record called google. DomainKeys and assign the values generated in the first step to it. It should appear as follows: v=DKIM1; k=rsa; p=ALb9a358abcAbcjslqRtsxdDAB

4. To save the changes, click the Save button.

How to check if DKIM has been configured in Google Console?

To check that your email has been configured, go to [Google Workspace Mx Control](#), search your domain's name in the search box, and click Run Checks. You will see a report that confirms you have your DKIM setup.

How to add DKIM records in Microsoft Office 365?

1. login to your security.microsoft.com/dkimv2
2. Click on Policies & rules -> Threat Policies ->DKIM
3. select the domain from which you are sending mails
4. Then, Click Create DKIM keys.
5. A pop-up will appear named Publish Cname, Click Copy.

This is an example of how DKIM records will look like

Name: selector1._domainkey

Value: selector1-your_domain-com._domainkey.your_domain.onmicrosoft.com

Name: selector2._domainkey

Value: selector2-your_domain-com._domainkey.your_domain.onmicrosoft.com

which can be broken into

Name	Type	Value
selector1	CNAME	selector1-your_domain-com._domainkey.your_domain.onmicrosoft.com

selector2	CNAME	selector2-your_domain-com._domainkey.your_domain.onmicrosoft.com
-----------	-------	--

1. Now log in to your Domains hosting provider
2. Go to DNS records management
3. Create a new DNS Record - Type: Your CNAME – Enter the DKIM key's name and value.

Then go back to your Microsoft 365 security centre and Enable the DKIM. And wait for a few minutes.

How to check if DKIM has been configured in Microsoft Office 365?

After adding Dkim records, you should verify that you have configured DKIM records successfully. To check whether you have successfully configured DKIM go to [MxToolbox](#) and fill in the domain name and selector1. Then Click on DKIM lookup.

You will see that you have successfully configured Selector1 . Now repeat the same process by changing selector1 to selector2 and clicking DKIM lookup.

Now you have successfully configured DKIM.

References

- <https://postmarkapp.com/guides/dkim>
- <https://www.sparkpost.com/resources/email-explained/dkim-domainkeys-identified-mail/>
- <https://www.kimbley.com/blog/31/3/2015/how-to-setup-spf-dkim-and-dmarc-in-g-suite>
- <https://www.agari.com/email-security-blog/dkim-setup/>
- <https://lazyadmin.nl/office-365/configure-dkim-office-365/>
- <https://www.alitajran.com/configure-dkim-record-for-office-365/>

Revision #4

Created 19 October 2023 01:19:52 by Admin

Updated 19 October 2023 05:02:05 by Admin