Email Security

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/

Dmarc Records

Domain-based Message Authentication, Reporting, and Conformance (DMARC) is an email authentication protocol that is designed to give email domain owners the ability to protect their domain from unauthorized use, commonly known as email spoofing. The purpose and primary outcome of implementing DMARC is to protect a domain from being used in business email compromise attacks, phishing emails, email scams, and other cyber threat activities.

Develop a DMARC Policy

Before you add a DMARC record, decide on the policy you want to enforce. There are three types of DMARC policies:

- `none`: Treat the mail the same as it would be without any DMARC validation.
- `quarantine`: Treat the mail as suspicious. Depending on the recipient's email server, this typically means the email is placed in the spam/junk folder.
- `reject`: Completely reject the email; it will not be delivered to the intended recipient.

Create Your DMARC Record

A DMARC record is a TXT record in your DNS that looks something like this:

```
v=DMARC1; p=none; rua=mailto:dmarc-@example.com; ruf=mailto:dmarc-failures@example.com; fo=1;
```

This example tells email servers that:

- `v=DMARC1` indicates the DMARC version.
- `p=none` is the policy (none, quarantine, or reject).
- `rua=mailto:dmarc-reports@example.com` is where to send aggregate reports of DMARC failures.
- `ruf=mailto:dmarc-failures@example.com` is where to send forensic reports of individual failures.
- `fo=1` tells the receiving server to generate reports if both SPF and DKIM fail.

Access Your Domain's DNS Settings

- Log in to the domain management console or control panel provided by your domain registrar or hosting provider.

Navigate to DNS Management

- Find the section where you can add DNS records. This might be called "DNS Management," "Name Server Management," or "Advanced Settings."

Add the DMARC Record

- Select the option to add a new DNS record.
- The type of record you will be adding is a TXT record.
- In the "Name" or "Host" field, enter "_dmarc". This will make the full hostname of the record "_dmarc.yourdomain.com."
- In the "Value" or "Data" field, enter your DMARC policy (like the example given in Step 2).
- Set the TTL (Time To Live) as advised by your DNS provider. The default is often 1 hour (3600 seconds), but if you're uncertain, 24 hours (86400 seconds) is a safer choice.

Save the Record

- Save the new record. DNS changes can take anywhere from a few minutes to 48 hours to propagate worldwide.

Test Your DMARC Record

- Use a DMARC record checking tool to ensure your DMARC record is valid. Many of these tools can be found online for free : Mxtoolbox
- Enter your domain and run the test. The tool should show your new SPF record.

Setting up DMARC is a proactive measure against email spoofing and phishing—it's not an instant fix, but it's an important part of a comprehensive email security strategy. Keep tweaking and monitoring, and you'll be on the right track to keeping your domain's reputation clean and your emails landing where they should.

SPF Records

The Sender Policy Framework (SPF) is an email authentication method designed to detect forging sender addresses during the delivery of the email. SPF allows the receiving mail server to check during mail delivery that a mail claiming to come from a specific domain is submitted by an IP address authorized by that domain's administrators. Adding an SPF record to your DNS configuration can help to reduce spam and improve email deliverability.

Step-by-Step Guide:

1. **Log In to Your DNS Provider's Control Panel:**
   - Access your DNS provider's website.
   - Enter your login credentials to access the DNS management console.
2. **Navigate to DNS Management Section:**
   - Look for sections like 'DNS Settings', 'Name Server Management', 'DNS Configuration', or similar.
   - Select the domain you wish to add an SPF record for if you have multiple domains.
3. **Access the DNS Records Section:**
   - Once in the DNS management area, locate the option to view or edit DNS records.
   - This area might be called 'DNS Records', 'Zone File Settings', 'Advanced DNS'.
4. **Check for Existing SPF Records:**
   - Before adding a new SPF record, ensure there are no existing SPF records for your domain to avoid conflicts.
   - An SPF record will start with "v=spf1". If one exists, you should edit this record instead of creating a new one.
5. **Add a New SPF Record:**
   - Look for an option to 'Add Record' or 'Create New Record'.
   - Select the type 'TXT' from the dropdown menu or record type options.
6. **Fill in the SPF Record Details:**
   - In the Host/Name field, you might enter "@" or your domain name to indicate the record is for the root domain.
   - In the Value/Text field, enter your SPF record, which starts with "v=spf1". Here is a simple example:

     ```
     v=spf1 ip4:123.45.67.89 include:_spf.example.com ~all
     ```

   - "**ip4**" defines the IP address authorized to send emails from your domain.
   - "**include**" is used to authorize emails from the domain specified (necessary if you're using a third-party service to send emails on behalf of your domain).
   - "**~all**" indicates that emails from your domain should only come from the specified sources, but it allows for soft failures (used for transitioning and troubleshooting).
7. **Set the TTL (Time to Live):**

- TTL determines how long the record is cached by resolvers. The standard is 3600 seconds (1 hour), but you can set this according to your preferences and needs.

8. **Save the Record:**
    - Click 'Save', 'Add Record', or 'Update' to save the new SPF record.
    - It might take some time for the changes to propagate across the internet, typically from a few minutes to 48 hours.
9. **Verify the SPF Record:**
    - Use online tools like **MXToolBox** to verify that your SPF record is published correctly.
    - Enter your domain and run the test. The tool should show your new SPF record.

Conclusion:

You have now added an SPF record to your domain's DNS settings. This should improve your email deliverability and protect against email spoofing. Remember to update your SPF record if you change your email service provider or add new services that send emails on your behalf.