Imagine two scenarios. In one, you are sending very important email to your potential customers, but you don't hear back from them. Later on you learn that this happened because your email went to spam folders and potentially you have lost business opportunities. In second scenario, you are receiving a call from your partner "what kind of emails you are sending"? But you have not sent any emails – someone impersonated you.

Both scenarios are real-life threats. And if you are using email service using your own domain, then you will probably want to ensure that setup is right so that you won't encounter such issues. Email providers should have domain setup verification procedures set up on their side, but sometimes they can fail or provide false positives. Additionally – it is always good idea to expand your knowledge. So let's dive into few technical terms regarding email setup for your custom domain: that is MX, DKIM, SPF and DMARC.

How Hackers Can Use a Domain Without Keys to Forge Emails

The absence of the SPF and DKIM records simply means that your domain is at risk of being attacked by a hacker. First and foremost, it is a good ground for hackers to convert your authentic emails to spam, and at the same time, they are easily forged. When they want to impersonate your emails they will use one of the free online SMTP servers and then modify it in their desired way in the 'FROM' field that sends it. For this reason, having proper records for your domain is for security reasons and a means of email verification. By using DMARC digital signature, hackers possibly cannot send emails on your domain's behalf, and then, again, the encryption cannot be forged hence securing your email not marked as spam.

Email Related Domain Records

Let's start from the very basics. Have you ever asked yourself who directs your internet traffic? The answer is: on the domain records. They inform the internet of the location that it should send the traffic to your internet. The most common records are the A records, CNAME records, TXT records, NS servers records, and MX records. In other words, domain name records serve as a contact book for the internet that keeps individual addresses. The distinctions are based on the conversion of human language to a machine language known to computers in the

form of IP addresses. For instance, you may not have memorized the numbers of people in your phonebook, yet you know their names, you will only look for the name and the number pops up. That is how domain records work for the internet. Therefore, when you search for a site in your browser, your gadget will employ domain records to identify the domain's IP address.

For email related purposes we will need just a few of them:

- A record or records to point to proper IP address of email server
- MX record to define domain where email is being processed
- TXT records for setting up DKIM, SPF and DMARC
- SRV records to make email setup easier

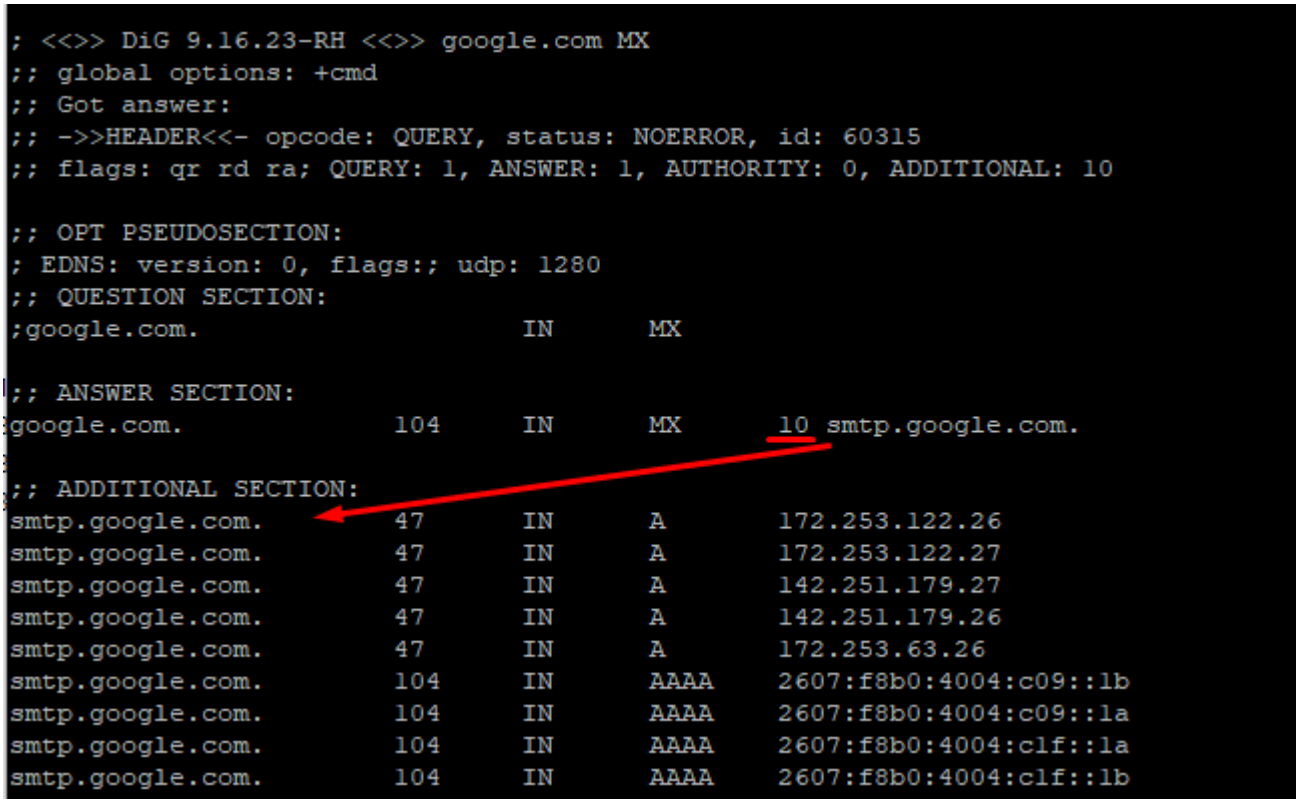
A and MX records are absolutely necessary to make basic email configuration work. But without DKIM, SPF and DMARC many email servers will reject your messages. And SRV is optional, but recommended – it will help your end users to set up email clients semi-automatically.

MX and A Records – Base For Setting Up Email

MX is short for Mail Exchange record. It is responsible for the identification of the individual servers that receive emails for the domain names. In other words, it is the MX records that are important in the email delivery to your address. To put it plainly, the MX records are used to inform the world mail servers that accept mail for a particular domain and also show where emails sent to the domain are routed. Therefore, an MX record is an entry in the DNS that guides the sending server on where to send the email.

If you want to check MX records on windows, open Windows Command Line. When terminal is up, you should type 'nslookup' and hit 'Enter'. It will ask you to type in your domain name. At this point, your MX record will be displayed after hitting 'Enter'.

On Linux, for identification purposes, it is achievied using dig tool from linux command line. Sample output *dig google.com MX* will look like this:



```
; <<>> DiG 9.16.23-RH <<>> google.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60315
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 10

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;google.com.                    IN      MX

;; ANSWER SECTION:
google.com.             104     IN      MX      10 smtp.google.com.

;; ADDITIONAL SECTION:
smtp.google.com.        47      IN      A       172.253.122.26
smtp.google.com.        47      IN      A       172.253.122.27
smtp.google.com.        47      IN      A       142.251.179.27
smtp.google.com.        47      IN      A       142.251.179.26
smtp.google.com.        47      IN      A       172.253.63.26
smtp.google.com.        104     IN      AAAA    2607:f8b0:4004:c09::1b
smtp.google.com.        104     IN      AAAA    2607:f8b0:4004:c09::1a
smtp.google.com.        104     IN      AAAA    2607:f8b0:4004:c1f::1a
smtp.google.com.        104     IN      AAAA    2607:f8b0:4004:c1f::1b
```

In both cases we are asking *Internet* (technically: your default DNS provided by your ISP or selected by you manually) *what is the MX record on domain google.com?*. As result you get not IP address, but rather name: *smtp.google.com* – but then there is additional section. And in this additional section there are 4 IPv4 addresses that domain *smtp.google.com* actually points to. Arrow on screenshot visualizes this idea. Instead of pointing to A record, MX record can point to CNAME record, but in the end if you follow CNAME record, you will end up with another A record that points to IP address – which is what we are ultimately looking for.

SPF Key and its Details

Spammers are all over the internet. They can endeavor their activities by sending spam emails on behalf of a domain. To prevent the vice, SPF is used to give permission only for specific servers to send emails. Therefore, an SPF is a technique employed to cushion domains from unverified emails purported to have been sent on their behalf. Additionally, with SPF utilization, a firm can list down verified and valid email servers. Originally, the SPF was known as ‘Sender Permitted From’, however with time it changed to ‘Sender Policy Framework’.

Nevertheless, the world has witnessed tremendous advancements since SPF resulting in improvements such as DMARC and DKIM, but SPF still plays an important role in the determination of email compliance. In this case, one of the importance of the SPF record is that it prevents email forgeries, so by adding SPF to your domain you are protected from others intruding on your domain.

Receiver server compares SPF domain record with domain from received email. If it notes any mismatch and discrepancies, it filters them and, at the same time, marks them as unauthorized hence rejecting them or just marking them as spam. In example:

> v=spf1 a mx include:send.sailingbyte.com ip4:188.68.224.153 -all

You can find whole explanation on great tool – mxtoolbox Sailing Byte sample – but in short this record is saying what records are authenticated (A, MX, additional domain and additional IP address) and what should destination server do if there is mismatch (-all means it should be discarded). So, the main information is that the SPF keys contain is the list of all authentic IP addresses (or domain records) that can send emails on behalf of your domain.

DKIM and the Information it Contains

This is yet another email authentication method that allows to detect unverified emails and helps servers mark them as spam or unauthorized. In the real sense, it is designed to identify mail that originates from a server that holds encryption key. For the Domain Keys Identified Mail to achieve its objective, it uses a concept known as Digital Signature affixation by using public key cryptography.

Public key cryptography is using two complimentary keys: one key is called *private* and should always be kept secure. It is used to sign original message or to decrypt incoming message, that was encrypted using public key. Second key is *public* – it is used to verify signature or to encrypt message that can only be decrypted using private key.

So when sender server receives request to send email in behalf of user, it is using private key to sign message and adds digital signature to the headers of email. The information in the header included the tag value parts like ‘d=’ in the case of the

signing domain and ‘b=’ for the actual signature. Now, when receiving server wants to validate this message, it can use known public key (that is held in TXT record of domain, so it’s available to everyone), to verify digital signature included in email headers. So by verifying the signature on the email received they can confirm the authenticity of the email as validly sent from the sender or a particular domain. Additionally it is proof that the email contents have not been tampered with since the signature affixation has been included. Therefore, DKIM allows the endorsement of a message by a signature and gives a platform for the sending organization to share information as to which emails are authentic or legitimate.

However, it does not single out abusive behavior or disclose it. The importance of DKIM at an organizational level is to form the basis of claiming responsibility for email messages sent out by the users. But if you have malicious users that use your email server to send authenticated emails to many receipients, you either should be able to identify such users either by using proper DMARC records (described below) or by adjusting your settings and limits for outgoing messages (which is outside of scope of this article).

And what DMARC record is for?

Until recently, DMARC record was not very widely used, but more and more mail servers require that it is present to actually deliver email and not block it. DMARC is kind of reporting information: so if mail server receives forged email, they can send automated report to postmaster (owner of the domain or designated email server administrator) saying “watch out, there are spammers trying to use your domain” or “watch out, some of your users is sending spam messages”. So on one hand, it is worth having such email. On the other hand, there can be a lot of information technical information involved, and in DMARC record certainly should NOT contain your private address – as DMARC records are available over the Internet without any protection. DMARC sample would look like this:

```
v=DMARC1; p=none; rua=mailto:dmarc@yourdomain.com
```

Because of that you may want to look to automate some of this reporting. Maybe an N8N DMARC automation flow would be a good thing for you to try out?

SRV and Other Records to Automate Email Setup

SRV records, or Service Location (DNS SRV) resource records play a crucial role in automating the email configuration setup process. These DNS entries provide information about services available within a domain and specify how to reach them. For instance, when configuring an SMTP server for sending emails, an administrator can utilize SRV records to automatically discover the appropriate mail servers without manually specifying IP addresses or ports. An example of such an SRV record might be:

```
_smtp._tcp.example.com IN SRV 10 5 443 smtpserver1.example.com
```

which indicates that there is a SMTP service available on TCP port 443 at `smtpserver1.example.com`. Similarly, for receiving emails via IMAP or POP3 protocols, corresponding SRV records can be defined to streamline the setup process. This automation not only reduces configuration errors but also enhances scalability and maintainability in large email infrastructures. For IT department it is very convenient, becuse end users (using Thunderbird for example, which I strongly recommend) will automatically detect server settings – and users only need to provide email and password.

In addition to SMTP services, SRV records are equally beneficial for configuring other mail-related services such as submission (for secure submissions), management (for administrative tasks), and authentication mechanisms like OAuth2 or SASL. For example, an administrator might define *_submission._tcp.example.com IN SRV 10 5 587 smtpserver2.example.net* to specify the server for submitting emails securely over TLS on port 587. This approach ensures that all email clients and servers within a domain can automatically discover and connect to the correct services, enhancing reliability and user experience. Furthermore, by leveraging SRV records in conjunction with DNSSEC (Domain Name System Security Extensions), organizations can add an extra layer of security to their mail infrastructure, protecting against man-in-the-middle attacks and ensuring that only authorized clients access email servers.

Similarly, you can set up autodiscover record. You need to create a DNS record (typically a CNAME or A record) pointing to the service of your email provider. This allows email clients, such as Microsoft Outlook, to automatically locate the

necessary settings for connecting to the mail server.

Summary – How Domain Setup Affects Your Business

It is important to use SPF and DKIM more, especially if you are an organization that sends commercial transactional details via mail. It is crucial to have SPF and DKIM to maintain a good relationship with your clients. Thanks to that they can perceive you as a serious business partner who keeps them away from loss and inconvenience caused by spoofing and scammers. Particular mail managers and administrators may have their own rules and regulations. However, if you are a serious organization with standard email protocols, SPF and DKIM are an integral part of your business operations. Understanding the security and authenticity of systems is part of understanding the needs of a domain name and all that domains incorporate. You can rely on Sailing Byte for more help in not only securing your domain but also all that relates to domain systems.