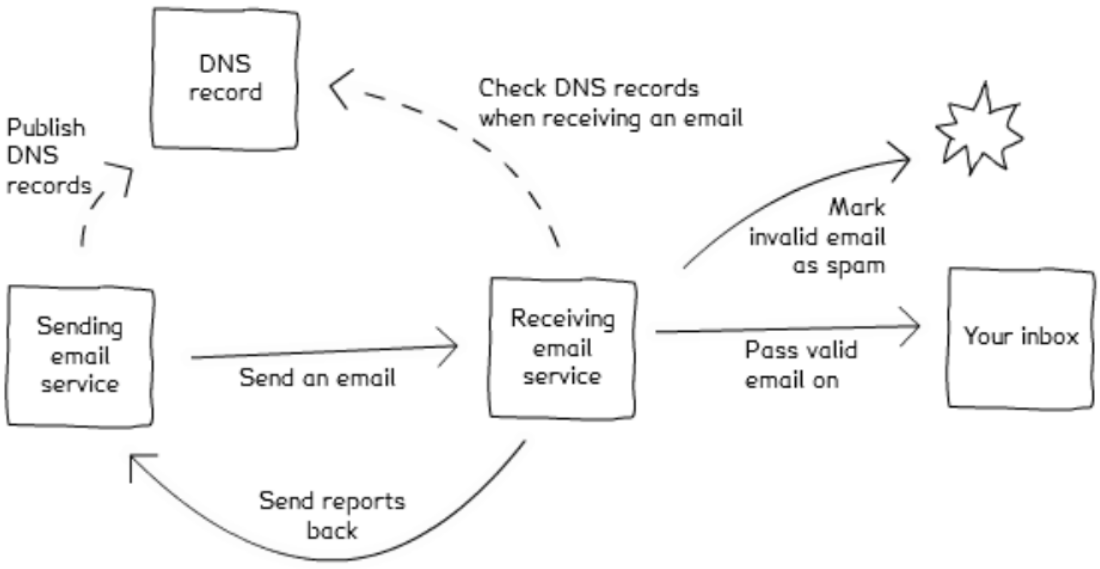
DMARC

Phishing is a systemic risk which impacts everyone. Phishing is a social engineering attack in which a fraudulent email message is sent and appears to be coming from a legitimate organization or user. The goal of this attack is to either steal personal identifiable information (i.e. usernames, passwords, bank or credit card information), to orchestrate fraud (false wire transfer requests) or to infect systems with malware, such as ransomware or a keylogger.

One difficulty for users when it comes to phishing is to determine whether or not the message came from a legitimate organization. Did the email come from a government agency, your bank or insurance company? Spammers are able to spoof the "From" address on mail messages, resulting in the recipients trusting the mail message. DMARC is a solution which can prevent this and help to remove email fraud.

What is DMARC?

DMARC (Domain-based Message Authentication, Reporting & Conformance) is an email authentication protocol, which includes a reporting function that allows senders and receivers to improve and monitor protection of the domain from fraudulent email. Implementation of DMARC will prevent Spammers from spoofing the "From" address on mail messages. Depending on the DMARC policy settings, any mail messages originating from an unauthorized mail server will be either quarantined or rejected. Thus leading to all spam and phishing messages using an organizations domain name will be quarantined or deleted before they reach their destination (employee or home user). The reports generated can then be used for intelligence or possible for law enforcement (if the activity is criminal in nature) purposes.



(Image Source: Gov.UK[1])

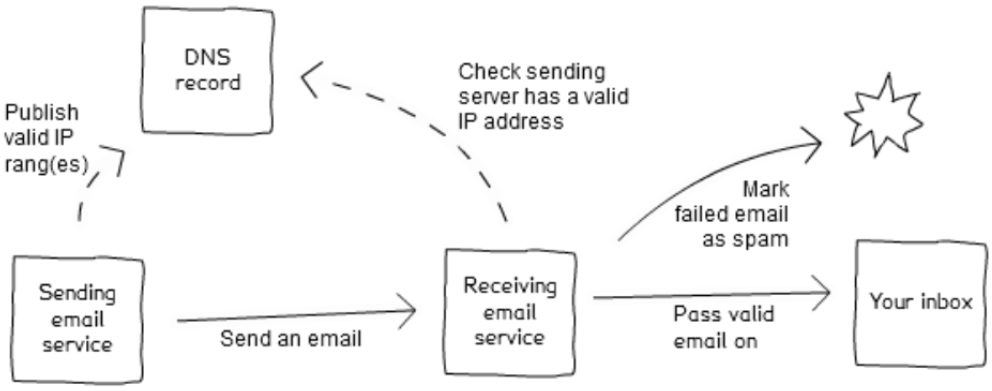
DMARC builds upon the existing authentication protocols SPF and DKIM. DMARC policy is triggered when SPF and DKIM both fail to yield authentication that is relevant to the "From" address of a given piece of email. The DMARC

1 Guidance: Domain-based Message Authentication, Reporting & Conformance (DMARC) - https://www.gov.uk/government/publications/email-security-standards/domain-based-message-authentication-reporting-and-conformance-dmarc

policy will not be triggered unless a message fails SPF and/or DKIM checks. DMARC relies upon these technologies to ensure integrity of the mail messages.

What is SPF?

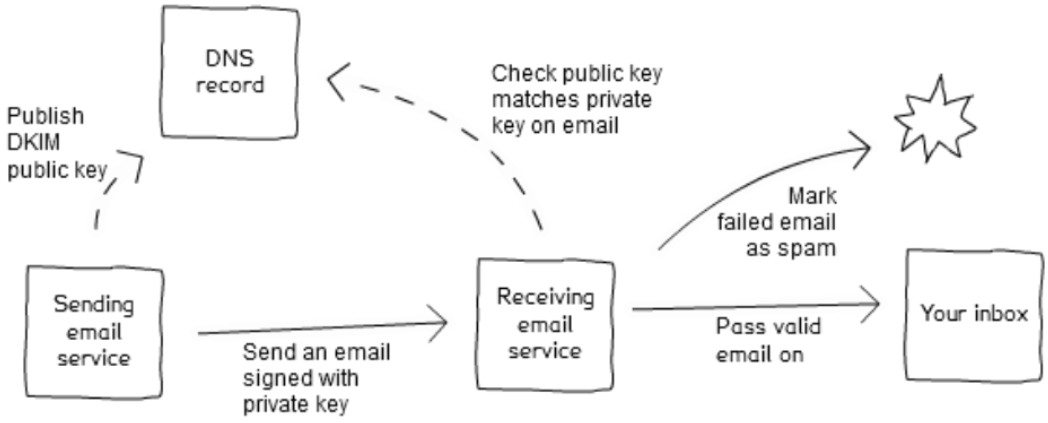
SPF stands for Sender Policy Framework. This policy is responsible for preventing the sender address from being spoofed. This is done by defining which mail servers are authorized to send mail on behalf of the organization's domain. If the mail server is not defined in SPF then the message is rejected or bounced.



(image source: Gov.UK[2])

What is DKIM?

DKIM stands for DomainKeys Identified Mail. DKIM is a mechanism designed for the purpose of validating a domain's identity that is associated with a mail message by using authentication that uses asymmetric cryptography. Basically, DKIM will authenticate a mail message by adding a digital signature to the message header. It is important to note that DKIM does not filter mail messages. It will allow for SPAM filters to determine the authenticity of the mail message being sent.



(Image Source: Gov.UK[3])

2 Guidance: Sender Policy Framework (SPF) - https://www.gov.uk/government/publications/email-security-standards/sender-policy-framework-spf

3 Guidance: DomainKeys Identified Mail (DKIM) - https://www.gov.uk/government/publications/email-security-standards/domainkeys-identified-mail-dkim

How to Implement these Protocols?

All three components rely on DNS and Mail Servers (MTA) to function. DNS will contain the policies to use, and the Mail Servers (MTA) are used for sending and verification of mail messages being sent.

SPF:
SPF is implemented by creating a TXT record in DNS. This TXT record will look similar to the following:

v=spf1 include:_spf.google.com ~all

The above is an example SPF TXT record if the organization is using Google Apps for email.
Please note, that if you are using a vendor for email cloud security, you should work with them to determine the appropriate settings for the SPF record.

The parts of the SPF record mean the following:

v=spf1	The TXT record will always begin with this. This defines the version of SPF being used. Currently SPF version 1 is the only available version
mx	If this is included, then the incoming mail servers (MXes) of the domain are authorized to also send mail for that domain
a:<domain>	This part should only be included if there are other systems, other than the mail servers, authorized to send mail for the domain.
include: <external domain>	Everything considered legitimate by a trusted external domain is legitimate for the organization's domain.
< - | ~ | ? | + > all	This part is always at the end. It will define how strict the servers should be when treating emails. Options: "-all" means only the domain's mail servers (and those in the 'a' and 'include' sections are allowed to send mail for the domain. All other are prohibited. "~all" only the domain's mail servers (and those in the 'a' and 'include' sections are allowed to send mail for the domain, but is in transition. All other are prohibited. "?all" means explicitly that nothing can be said about validity. "+all" means that any host can send mail for the domain. This should never be used.

Additional parts of SPF can be found at the Sender Policy Framework using the following link: http://www.openspf.org/SPF_Record_Syntax.

Once the TXT record for SPF is created, then make sure to confirm that it is working correctly. This can be done by using multiple SPF testing tools online. Dmarcian.com provides an online tool called SPF Survey (https://dmarcian.com/spf-survey/) or you can use tools provided by OpenSPF.org (http://www.openspf.org/Tools).

DKIM:
Please note, that if you are using a mail message provider, you must follow the procedures provided by them to setup DKIM correctly.

The following are steps to setup and utilize DKIM:

1. Create an inventory of the organization's sending domains. DKIM will need to be set up for each domain within the organization for proper authentication.
2. Install and configure DKIM on the organization's email server
    a. If you are using a mail provider, then make sure to follow the steps provided by the provider.
3. Create the DKIM keys:

    DKIM has two parts, the private key and public key. Creating the keys for DKIM will vary depending on who is providing email services to your organization.

    If you are using an external service for both mail and DNS, then the mail provider will need to provide you with the public key. This public key is then published as a TXT record in DNS. Most DNS providers limit the size of the TXT record to 255 characters, so you may have to work with the provider to increase the size or create the TXT record. The private key is held by the mail provider and typically not provided to the organization.
    If the organization has its own email server, then the DKIM keys must be generated by the IT staff (or the one responsible for DKIM implementation). There are multiple DKIM key generators available on the Internet. If you choose to use one of these, just make sure that you have the option to delete the key after it is generated and copied to files on your end.

    To create the keys without a third party, an open source project called opendkim (http://www.opendkim.org/) is available. Opendkim contains various tools to assist with creating the DKIM key.

    Another option is to use OpenSSL to generate the DKIM keys. This can be done by using the most recent version of OpenSSL and typing the following command for the private key:

    openssl genrsa -out dkim-private.pem 1024 -outform PEM

    This will generate a private key file called dkim-private.pem. Next, type the following command to generated the public key:

    openssl rsa -in dkim-private.pem -out dkim-public.pem -pubout -outform PEM

    This command will generate the public key (dkim-public.pem) based off of the previously created private key (dkim-private.pem).

4. Move the DKIM Private Key in the location specified by the DKIM installation in step 2. Make sure it is in a folder with restricted access.
5. Publish DKIM Public Key. This is done by creating a TXT record on the DNS server.

    The TXT record will look similar to the following:
    mail._domainkey IN TXT "k=rsa;
    p=MHwwDQYJKoZIhvcNAQEBBQADawAwaAJhAKJ2lzDLZ8XlVambQfMXn3LRGKOD5o6l;"
    Sections:

- mail._domainkey – name of the DKIM key in DNS. Any name can be used before the ".", however it must end with "_domainkey".
- IN TXT – defines this is a TXT record (only used if manually creating a TXT record in DNS)
- k=rsa – defines key algorithm used (always RSA)
- p=<key string in public key file generated previously> – defines the public key string

Optional Section:

- v=DKIM1 – defines DKIM version

6. Configure email server to use DKIM.
7. Confirm DKIM is working.

DMARC:

Just like SPF and DKIM, DMARC utilized a DNS TXT record for implementation. The TXT file will be "_dmarc.<FQDN>". The record will contain information similar to the below:

v=DMARC1; p=quarantine; rua=mailto*:<email address>*; ruf=mailto*:<email address>*; fo=1; adkim=r; aspf=r; pct=100; rf=afrf; ri=86400; sp=quarantine

Here are common tags used in DMARC TXT records[4]:

Tag Name	Required	Purpose
v	required	Protocol version
p	required	Policy for domain. Options are: • None – no action taken, but recorded in the DMARC report. • Quarantine – mail message is marked as spam. • Reject – message is deleted.
rua	optional, but recommended for analysis and monitoring purposes	Reporting URI of aggregate reports. Reports can be sent to multiple addresses. Each email address will start with "mailto:" and separated using a comma.
ruf	optional, but recommended for analysis and monitoring purposes	Reporting URI of failed reports. Reports can be sent to multiple addresses. Each email address will start with "mailto:" and separated using a comma.
fo	optional	Defines error reporting policy. If not defined, defaults to 0 (Generate report to the sending MTA if all underlying checks failed). Other values are: • 1 - Generate report to the sending MTA if any underlying check failed. • d – Generate a report if DKIM check fails • s – Generate a report if SPF check fails Multiple values can be used by using a colon as a separator.

4 Google Support – Add a DMARC record - https://support.google.com/a/answer/2466563?hl=en

adkim	optional	Alignment mode for DKIM. Options are: • r (relaxed) – default if not defined. Allows for any subdomain defined in the DKIM header. • s (strict) – the sender's domain name must match the domain in the DKIM header exactly.
aspf	optional	Alignment mode for SPF. Options are: • r (relaxed) – default if not defined. Allows for any subdomain. • s (strict) – the organization domain name in the MAIL FROM command (in SMTP) and the from: header (in the mail item) must match exactly
pct	optional	% of messages subjected to filtering by the DMARC policy. Can be any number from 1 to 100. Default is 100, which is all messages.
rf	optional	Defines the format of the reports generated. Format values are: • afrf – default value if not defined. Format is defined by RFC 5965. • iodef – Format is defied by RFC 5070.
ri	optional	Defines the reporting intervals in seconds. Id not defined, the default is 86400 seconds, or 24 hours. Please note, that reports are not guaranteed to be sent receiving MTAs. Reports are sent on a best effort basis.
sp	Optional	Policy for subdomains of the domain. If this tag is not present, then the policy will follow the option set for the p tag for all subdomains.

Best practice is to start with none and slowly work your way up to reject. This is to make sure that any legitimate mail messages are not being dropped due to the DMARC policy.

The DMARC Report

Once the DMARC policy is implemented with the rua and/or ruf tags, aggregate reports (in XML format) will be generated containing information about which mail messages pass/fail against SPF and DKIM. This provides visibility into possible authentication issues and/or spam activity for your organization.

The reports contains the following[5]:

1. ISP Information
2. Line-by-line description of your organizations DMARC record
3. Summary of authentication results

It is important to note, that these reports will not come from just one source. You could potentially receive 10 to 100 (possibly more) reports on a daily basis (number of reports generated is dependent on amount of emails sent). This will make it difficult to manually review each report, especially since it is in XML format and some reports could be lengthy. Another item to take note of is that not all receivers will send failure reports. So there is a chance that you may not receive any forensic reports. This is due privacy and data sharing regulations across nations.

These reports can be made human readable by developing an XML converter or by working with a commercial vendor. Most commercial vendors will provide a backend repository that will make the reports human readable as well as provide various levels of analysis and guidance.

5 How to Read Your First DMARC Reports (Part 1) by Amy Gorrell - https://blog.returnpath.com/how-to-read-your-first-dmarc-reports-part-1/)

Additional Resources

DMARC.org (http://www.dmarc.org) - Best source for DMARC information.

Dmarcian.com Tools:

- DMARC Inspector (includes a DMARC Record Wizard): https://dmarcian.com/dmarc-inspector/
- SPF Survey: https://dmarcian.com/spf-survey/
- DMARC Status: https://dmarcian.com/dmarc-status/

DMARC Creation Wizards:

- ReturnPath: https://stopemailfraud.returnpath.com/dmarc-start/?_ga=1.57923690.1397602122.1460466044
- Kitterman Techincal Services: http://www.kitterman.com/dmarc/assistant.html
- Agari: https://app.agari.com/dmarc/record_creator

SPF Creation Wizards:

- SPF Wizard: http://www.spfwizard.net/
- Dynu: https://www.dynu.com/NetworkTools/SPFGenerator
- xNode: https://xnode.org/page/SPF_Record_Creator
- SPF Record: http://www.spf-record.de/generator

DKIM Creation Wizards:

- DKIM Core: http://dkimcore.org/tools/keys.html
- Port25: https://www.port25.com/support/domainkeysdkim-wizard/
- DKIM.org: http://dkim.org/deploy/

DMARC/SPF/DKIM training:

- DMARC - Overview
- DMARC - How It Works
- DMARC - Benefits
- DMARC - Return on Investment
- DMARC - Deployment Process
- SMTP Overview
- SPF Overview
- DKIM Overview
- DMARC - Technical Overview