Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Protect domains against phishing

Restrict e-mail spoofing with SPF, DKIM and DMARC

Guide | Version 2.0 | December 2023

Prevent e-mail spoofing and phishing by protecting your domains with e-mail authentication. Phishing involves sending e-mails with misleading content to get the recipient to download malicious software or divulge information. Attackers resort to a range of techniques to improve their chances of success. Falsifying domain names ('spoofing') is one such method. Spoofing makes it more difficult for recipients to recognise phishing e-mails because it appears as if such e-mails were sent from the e-mail address of a reliable organisation. Organisations that do not protect their domain names against e-mail spoofing might cause damage to recipients due to abuse and suffer reputational damage themselves as a result. Moreover, it may harm the correct delivery of e-mail. Receiving mail servers increasingly block e-mails without e-mail authentication so recipients do not receive them.

The NCSC recommends protecting all of your organisation's domain names by means of e-mail authentication using SPF, DKIM and DMARC. Government organisations are obligated to implement SPF, DKIM and DMARC because these e-mail authentication protocols are on the 'apply or explain' list. For all other organisations, there is a strong recommendation to implement these standards.

Target group

E-mail administrators, DNS administrators, security officers.

Partners

The following organisations contributed to this guide: the Dutch Tax Administration (Belastingdienst), the Employee Insurance Agency (UWV) and Standardisation Forum.

Background

Attackers frequently use e-mail phishing to gain access to sensitive data or networks.[1] Attackers can choose from a range of techniques to mislead e-mail users. Phishing comes in many guises, with different influencing techniques being used to trick recipients. These include specifically targeted attacks by state actors using insider information ('spear phishing') or more generic attacks for financial purposes that target businesses ('business e-mail compromise'). Whatever variant might be used, phishing exploits the human factor in the chain of defence: the link with the highest chance of success.

'Spoofing' is one of the attack methods that can be deployed to improve the chance of success in phishing. Spoofing misuses the structure of the e-mail protocol. The domain name of the sender is not verified in the absence of e-mail authentication with SPF, DKIM and DMARC, so attackers can compile e-mails that appear to come from a reliable organisation. For instance, a user may receive a spoofed e-mail that appears to have been

[1] Please refer to the 2023 IOCTA report: https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202023%20-%20EN_0.pdf

sent from info@example.nl but actually comes from a malicious party.

As such, it is difficult for the recipient to recognise phishing e-mails when spoofing is used as an attack technique. Moreover, it has a damaging impact on the organisation that owns the domain name that was misused. It is possible that e-mail providers classify the organisation as an originator of phishing e-mai, and as a result legitimate messages could also be blocked. Apart from that it is bad for the organisation's reputation and may cause reputational damage.

The NCSC recommends protecting all of your organisation's domain names by means of e-mail authentication using SPF, DKIM and DMARC. The NCSC also recommends using SPF, DKIM and DMARC to filter incoming e-mail for phishing mail. This guide does not discuss these topics; you can find more information in other places.[2]

Government organisations are required to implement SPF, DKIM and DMARC. The Standardisation Forum conducts periodical measurements to check that government organisations are compliant.[3] A strong recommendation has been issued for all other organisations. The implementation of e-mail authentication is a good practice that many organisations now use.[4]

In addition to mail server administrators, bulk mail senders must also make authentic e-mail recognisable. The NCSC guide '*Good bulk mail does not look like phishing mail'* covers this.

Different attack methods

Spoofing is just one of the options used by attackers to improve the chances of success in phishing. Attackers can also buy look-alike-domains ('typosquatting'), send falsified text messages ('smishing'), or deploy QR codes to try and mislead users into visiting malicious websites. It is important to realise that in addition to e-mail authentication with SPF, DKIM and DMARC, e-mail users need tobe trained to recognise a range of phishing methods and know where to report suspicious e-mails.

Protect domains against spoofing

Effective phishing protection requires a multilevel approach that is tailored to people, technology and the organisation. This guide focuses primarily on protection against e-mail spoofing using e-mail authentication. You can do this with the aid of SPF, DKIM and DMARC, which we will explain below.

SPF

The Sender Policy Framework (SPF) is a protocol that allows a domain name owner to specify which mail servers are authorised to send e-mail on behalf of the domain name.[5] Receiving mail servers can use SPF to verify whether an e-mail was sent by an authorised mail server.

A SPF policy specifies which mail servers are authorised to send e-mail on behalf of a

[2] For more information, please visit: https://www.m3aawg.org/sites/default/files/m3aawg-email-authentication-recommended-best-practices-09-2020.pdf

[3] For more information, please visit: https://www.forumstandaardisatie.nl/metingen/informatieveiligheidstandaarden

[4] You can check your domain e-mail authentication here by doing the e-mail test at https://www.internet.nl/

[5] For technical specifications, please visit https://datatracker.ietf.org/doc/html/rfc7208

domain name. The policy is added to the DNS zone as a TXT record.

An SPF policy for the domain 'example.nl' can look like this:

example.nl. TXT "v=spf1 mx a:mail.example.nl ~all"

In this example, the policy specifies the following configurations:

- *v=spf1*: current SPF version.
- *mx*: inbound mail servers are also allowed to send e-mail.
- *a:mail.example.nl*: the mail server with this name is authorised to send e-mail. IPv4 and IPv6 addresses can also be included here.
- *~all*: Multiple options are available here. A hard fail is specified as a minus symbol (-). In this case, unauthorised e-mails are rejected. A soft fail is specified as a tilde symbol (~). Unauthorised e-mails can be flagged as suspect. Using ~all (soft fail) is usually the preferred option for sending domains. The reason is that if the SPF authentication fails with an SPF hard fail, an incoming mail server can already block the connection without reviewing the DKIM signature and DMARC policy. This can result in e-mails being blocked incorrectly.

An incoming mail server that verifies mail on the basis of SPF sends a DNS query to see whether the domain name of the sender's address has an SPF policy. In that case, it determines whether the outgoing mail server is included in the SPF policy. If the mail server is in the policy, the mail server concludes that the e-mail is authentic.

SPF can be used to filter incoming e-mail for spam and phishing mail. In and of itself, however, SPF does not provide effective protection against e-mail spoofing.[6] DMARC remedies this downside. Moreover, SPF also cannot handle e-mail forwarding. DKIM is necessary to supplement this.

Can the sender be verified?

A domain name owner can use SPF to specify what mail servers can send e-mail on behalf of a domain name. SPF is an important step in protecting against e-mail spoofing. It does not offer total protection, however. SPF must be used in combination with DKIM and DMARC if it is to combat e-mail spoofing effectively.

DKIM

Domain Keys Identified Mail (DKIM) is a protocol that allows a domain name owner to specify the key with which e-mails sent on behalf of the domain name must be signed.[7] Outgoing mail servers sign all outbound e-mail with this key on behalf of the domain name. Incoming mail servers can use DKIM to verify that an e-mail was sent by an authorised party.

DKIM is configured for outgoing e-mail by adding a TXT record to the appropriate DNS zone. Software on the mail server adds the actual signature to the e-mail.

The outgoing mail server adds the field 'DKIM-Signature' to the e-mail header. This field contains a digital signature for the e-mail's content (both in the headers and in the body).

[6] SPF uses the '5321.From header' field, which is generally invisible to the user. The sender address shown to the user ('5322.From header') is not used by SPF authentication, but DMARC uses it.

[7] For technical specifications, please visit https://datatracker.ietf.org/doc/html/rfc6376

The incoming mail server uses the sender's domain name (d) and a selector (s) from the DKIM Signature to transmit a DNS query. The selector field makes it possible to use different keys for a single domain name. In response, the mail server receives the sender's public key to authenticate the signature. If the check is successful, this means the e-mail was indeed sent by the domain name in question and it was not altered during transport. We also recommend that you consider configuring this for your subdomains (newsletter.example.nl), for instance if you allow other parties to send e-mail on behalf of your domain or use newsletters, and create specific DKIM keys for those purposes.

DKIM signatures

DKIM is used to add a digital signature to outgoing e-mails. The recipient of the signed e-mail checks the signature to verify the e-mail's authenticity and integrity.

Like SPF, DKIM offers receivers an additional opportunity to filter incoming e-mail. One disadvantage may be that the DKIM signature can be damaged if the message is altered during transport (mailing lists are an example). In addition to SPF and DKIM, effective protection against e-mail spoofing requires DMARC since attackers can simply delete the signature.

DMARC

Domain-based Message Authentication, Reporting and Conformance (DMARC) is a protocol that domain name owners can use to publish policies for handling e-mail that does not comply with the SPF or DKIM policy.[8] It is therefore a vital step in combatting e-mail spoofing. Without DMARC, the incoming mail server does not know what it has to do with e-mail that does not comply with the SPF or DKIM rules. DMARC includes the following features:

- *Feedback.* Incoming mail servers return a report (XML file) to the outgoing organisation when necessary (depending on how DMARC is configured). This allows the sending organisation to gain insight into the e-mails that are transmitted on behalf of their domain names. They can use this information to identify mail streams and improve how SPF and DKIM work.
- *Policy.* A DMARC policy instructs incoming mail servers in handling e-mail that does not comply with the SPF and DKIM policies of the sending domain name. Possible instructions are 'reject' (bin), 'quarantine' (tag as spam) and 'none' (accept).

In our 'example.nl' example, DMARC may look like this:

v=DMARC1; p=reject; rua=mailto:dmarc-authfail.example.nl; aspf=s; pct=100;

DMARC consists of a TXT record (_dmarc.example.nl) that is added to the DNS zone. This contains the following information:

- *v =DMARC1:* current DMARC version.
- *p*: what the incoming mail server must do with e-mail not complying with DKIM or SPF policy (*none, quarantine* or *reject*). We recommend using 'reject' as your policy.
- *pct*: The percentage showing to what section of the e-mail stream the DMARC policy must be applied. This is mainly used for testing, for instance if you want to move from p=none to p=quarantine or p=reject. If 'pct' is not included, the default setting is pct=100.

[8] For technical specifications, please visit https://datatracker.ietf.org/doc/html/rfc7489

- *rua*: The e-mail address to which receiving mail providers can transmit the DMARC report.
- *aspf=s*: the alignment level. The incoming mail server verifies that the sender address shown coincides with the domain specified in SPF (aspf) and DKIM (adkim). The value 'strict' ('s') ensures precise comparison, while 'relaxed' ('r') means that the mail server verifies that the sender address is included in the same domain. You can specify this by adding aspf or adkim with r=relaxed and s=strict. The default value is 'relaxed'.

Policy with DMARC

DMARC determines what an e-mail recipient must do with e-mails that do and do not comply with the SPF and DKIM rules. As such, it is the final step in effective protection against e-mail spoofing.

DMARC was designed for use in tandem with SPF and DKIM. If an e-mail does not comply with the SPF or DKIM policy, the e-mail is categorised as non-authentic. Correct configuration is vital here because the following situations might give issues:

- Domain names from which e-mails are sent to mailing lists. A mailing list administrator can configure it to prevent problems with SPF, DKIM and DMARC.[9]
- Automatically forwarded e-mails. These do not comply with the sending domain name's SPF. If an e-mail is not signed using DKIM, is it flagged as non-authentic.

Course of action

Phishing is still one of the most commonly used methods to gain initial access to networks or information. Attackers use persuasion techniques to exploit the human factor in cybersecurity behaviour. One frequently used method is to use e-mail spoofing. With e-mail spoofing it is harder for your customers, contacts or vendors to recognise phishing e-mails. By implementing SPF, DKIM and DMARC on all of your domains (including those that are not used for sending e-mail), you make it harder for the attackers to leverage e-mail spoofing from your domains.

Keep in mind that it is impossible to shield your customers from all phishing mail, so make sure that you explain clearly to your customers and partners how you communicate with them and what they can do if they do receive phishing e-mail on behalf of your organisation. It is a good practice to limit the number of domains you use to send e-mail to the minimum. You should also stimulate people to report phishing from your domain names and set it up so they can do this quickly and easily. Responding quickly to a phishing attack or attempt is vital to prevent further damage.

[9] Please refer to this page for more information: DMARC.org

Implementation strategy

1 ***Preparation*** Create a list of all domain names, e-mail streams and e-mail types. This overview contains both domain names that are used to send e-mail and domain names that do not send e-mail. A DMARC implementation, even without SPF and DKIM, can be used to map missing information. Analyse the collected information on the basis of your defined e-mail authentication targets, such as preventing unauthorised e-mail streams. This will help you identify problems and appropriate measures to solve them.

Technical guidelines:

- Create a DMARC record for every domain name. Initially use the value 'none' in your policy (for instance for a one-month period) and specify an e-mail address to which mail servers can transmit their reports.
- Use the reports to remedy e-mail streams that do not comply with the SPF and DKIM policies and correct 'identifier alignment' problems. This is also an opportunity to recognise e-mail that passes your SPF checks but does not comply with the DKIM policy. Clearly these e-mails will cause problems in case of forwarding. You can use tools to facilitate analysis.

2 ***Execution*** Implement your measures. This may involve new implementations or implementing necessary configuration changes. E-mail and DNS administration are responsible for this task.

Technical guidelines:

- *(In general)* Do not use DKIM but do use DMARC and SPF for inactive domain names or domain names that are not used to send e-mail. Configure these domains with SPF and DMARC, even if they are not used, to eliminate the possibility of e-mail spoofing via these domains.
- *(SPF)* Check that the SPF policy is added to domain names by searching for the TXT record in the DNS. Publish an SPF policy as a TXT record in the DNS zone of these domain names. Use a soft fail policy to prevent false positives. Also make sure that an SPF policy with the value ' v=spf1 -all' (hard fail) is included for all domain names that are not used to send e-mail to prevent misuse of these domain names. It is important to create an individual SPF record for every subdomain to prevent malicious players sending spoofed e-mails from real or falsified (sub)domains. Also note that it is important, when referring to an external mail service in the SPF policy (a so-called 'include:'), it is important for this service to check that the sender uses an authorised domain name to ensure that customers cannot send e-mail via one another's domain names (reject_sender_login_mismatch).[10]
- *(DKIM)* Generate public and private keys (at least 2048-bit RSA). Add the public key to the DNS zone of the domain name in question as a TXT record. Ensure that the Signing identity (d=) matches the From: header domain name exactly, similar to strict alignment in DMARC. Use a separate key pair and an individual selector for each organisation and generate new key pairs to create the DKIM signature on a regular basis, for instance biannually.[11]
- *(DMARC)* Ensure that the 'identifiers' are aligned for a successful Identifier Alignment check by DMARC. These are the fields used for authentication. The RCF5322.From domain name and the SPF and DKIM domain names must be identical. The 'Strict' mode requires an exact match; the 'Relaxed' mode requires a domain name match.
- *(DMARC)* Switch to a more stringent policy after the initial period. If all mail servers for a specific domain name are included in the SPF policy and all e-mail traffic is signed with DKIM, publish a 'quarantine' policy with a low 'pct' value. Debug false positives (for missed e-mail streams) and gradually raise the 'pct' value. If 'pct' is set to a value of 100 without deleterious effect, publish a 'reject' policy with a low 'pct' value. Repeat the debugging process and adjust the value. The objective is to authenticate the highest number of e-mail streams by including a 'reject' policy.

3 ***Check*** The implementation, configuration and use of the e-mail authentication methods must be monitored to ensure continued effectiveness. Look for misuse of domain names, problems with authorised senders, and mail server changes. The reports generated by DMARC may assist you in doing this effectively. Problems and measures are identified on a continuous basis. One tool you can use for testing is https://www.internet.nl

4 ***Adjust*** It goes without saying that the measures identified on a continuous basis in the previous step must actually be implemented.

[10] For an explanation of this vulnerability, please see https://doi.org/10.48550/arXiv.2312.07284

[11] Further details can be found at https://www.m3aawg.org/sites/default/files/m3aawg-dkim-key-rotation-bp-2019-03.pdf

Publication
National Cyber Security Centre (NCSC-NL)
P.O. Box 117, 2501 CC The Hague
Turfmarkt 147, 2511 DP The Hague
+31 (0)70 751 5555

More information
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

December 2023