Mail: DMARC - Protection against Spoofing and Phishing

What is DMARC?

DMARC (Domain-based Message Authentication, Reporting, and Conformance) is a **email authentication protocol**which protects domains against:

- email address impersonation (spoofing),
- phishing attacks,
- unauthorised use of the domain for sending e-mails.

DMARC works with two other message authentication mechanisms:

- **SPF** (Sender Policy Framework) - determines which servers can send emails on behalf of a domain.
- **DKIM** (DomainKeys Identified Mail) - a cryptographic signature in the message to confirm the authenticity of the sender.

How does DMARC work?

1. the recipient server (e.g. Gmail, Outlook) receives the email message. 2. checks that the message:

- has passed the **SPF**,
- passed the **DKIM**,
- and whether **the sender is aligned with the domain** (i.e. the so-called „alignment”).

3. based on the result, the server checks **DMARC policy**which is set by the sender's domain. 4. depending on the policy (`none`, `quarantine`, `reject`), the message is:

- accepted,
- marked as spam,
- or rejected altogether.

DMARC record in DNS

A DMARC record is **TXT record**, added to the DNS zone of a domain, e.g.:

```
_dmarc.ostrowski.net.pl. IN TXT "v=DMARC1; p=quarantine;
rua=mailto\:kacper\@ostrowski.net.pl
```

Syntax of the DMARC record

Parameter	Description
`v=DMARC1`	Protocol version (always `DMARC1`).
`p=`	DMARC policy (`none`, `quarantine`, `reject`).
`rua=`	E-mail address for aggregate reports
`ruf=`	E-mail address for forensic reports (rarely used)
`fo=`	When to generate reports (e.g. `fo=1` = any SPF/DKIM failure)

DMARC policies

p=none

* Monitoring mode. * Takes no action against unauthorised messages. * Used to collect reports and verify SPF/DKIM configuration. * Recommended as a first step.

p=quarantine

* Sends suspicious messages to the folder **SPAM/JUNK**. * Protection against phishing - but does not block messages completely. * Good compromise between security and risk of false positives. * Usually used as a second step before full rejection (`reject`).

p=reject

* Strongest policy - completely **rejects** messages that fail the tests. * Provides maximum protection against spoofing. * Recommended **only when**when:

- SPF and DKIM are correctly configured,
- You have full control over all servers sending messages on behalf of the domain.

Example DMARC Records

Monitoring mode

```
v=DMARC1; p=none; rua=mailto\:kacper\@ostrowski.net.pl
```

Quarantine mode

```
v=DMARC1; p=quarantine; rua=mailto\:kacper\@ostrowski.net.pl; fo=1
```

Rejection mode

```
v=DMARC1; p=reject; rua=mailto\:kacper\@ostrowski.net.pl; fo=1
```

Reporting (rua, ruf)

- **rua** - summary reports (once a day), in XML format, showing SPF/DKIM/DMARC statistics.
- **ruf** - detailed reports (if supported by the recipient), containing copies of problematic messages.

Reports can be analysed manually or with tools such as:

- https://dmarcian.com/
- https://easydmarc.com/
- https://mail-tester.com/
- https://mxtoolbox.com/

Recommended order of implementation

1. **Create and verify SPF and DKIM**. 2. **Add DMARC record with `p=none` and monitor reports**. 3. after a few days/weeks:

- if legitimate messages pass tests,
- and reports show no errors,

4. **Change policy to `p=quarantine`.**. 5. after the next testing phase, go to **`p=reject`.** (full protection).

Summary

DMARC is a key component of email security. It enables the domain owner to:

- reputation protection,
- prevention of spoofing and phishing,
- collection of diagnostic data,
- control over how unauthorised messages are handled.

Full protection requires correct configuration **SPF**, **DKIM** and a well-chosen **DMARC policy**.