



RESEARCH

Research among NOAB administration offices, 2026

A public count of DNS and HTTPS records at active NOAB offices

From 1 to 7 October 2026, 68.6% of the 854 unique domains of active NOAB offices did not ask receivers to block or quarantine fake mail. SPF is published at most offices. The gap is DMARC policy.

68.6% have no enforcing DMARC policy

31.4% ask receivers to reject or quarantine

62.4% SPF ends in -all

61 domains at 10 or more SPF lookups

854 unique domains. 893 offices with an own domain. 919 active offices in the public directory.

NovaMX B.V., Beverwijk

Census period: 1 to 7 October 2026

Published: 8 October 2026

Contents

What independent means here	3
1. Why this measurement.....	3
2. Population	3
3. Method	3
4. DMARC policy	4
5. RUA and RUF.....	4
6. SPF	5
7. SPF lookups and flattening	6
8. DNSSEC, HTTPS and transport.....	8
9. Regions.....	9
10. What this means for an office	11
11. Conclusions.....	12
12. What this measurement does not say	12
About NovaMX	12

What independent means here

NovaMX carried out this measurement itself. Nobody in the sector commissioned it, paid for the count, or saw the results before publication. The source is the public NOAB office directory, plus public DNS and one HTTPS request per own domain. Offices were not chosen because they are, or are not, NovaMX customers.

NovaMX also sells mail security, including DMARC reports and SPF flattening. That interest is stated here so a reader can weigh it. The figures in this report are counts, not an offer. No office is named.

1 Why this measurement

Administration and tax advisory firms send invoices, filings and payment requests in the firm's name. If an outsider can make a message look as if it came from that domain, a client may change a bank account because the sender looks familiar.

Whether that outsider succeeds depends partly on records anyone can query. SPF is the published list of systems allowed to send mail for the domain. DMARC is a separate instruction to the receiving mail server: what to do when a message fails that check, and where a report may go. DNSSEC protects the answers to those questions against forgery in transit. This report counts those public signals for one defined profession.

2 Population

NOAB is the Dutch association of administration and tax advisory firms and speaks of about 1,100 member offices. From 1 to 7 October 2026 the public office directory listed 919 active offices. That is the population of this report: a count of that list, not a sample from a larger file.

Of those 919 offices, 21 had no website in the directory, and 5 used an address on a platform or social network. That second group has no own mail domain to judge. That leaves 893 offices with an own domain, together 854 unique domains. Some offices share a domain. National mail figures are therefore per domain. Regional figures are per office: each office inherits its domain's score.

This report covers only the offices on that list. Offices that are not on it were not counted and are not compared here.

3 Method

For each own domain, from 1 to 7 October 2026, the following was requested, using ordinary DNS and one HTTPS connection to the published website:

- SPF on the organisational domain: the sender list, and how many DNS references (lookups) sit in the full chain.
- DMARC at `_dmarc`: the `p=` policy, and whether `rua` or `ruf` contains a `mailto` address for reports.
- Whether an MX record exists.
- Whether the parent has a DS record. That means DNSSEC is delegated, not that the chain validates.
- MTA-STS as a TXT `v=STSV1` at `_mta-sts`, and TLS-RPT as a TXT `v=TLSRPTv1` at `_smtp._tls`.
- Whether the published website has a valid TLS certificate, and whether a response sends HSTS.

A lookup in the SPF count is one of these terms: `include`, `a`, `mx`, `ptr`, `exists` or `redirect`, including when the term sits inside a nested `include`. `ip4`, `ip6` and `all` do not count. That is the same limit as in RFC 7208: at 10 or more of those

terms, a receiver may treat the SPF result as a permanent error. The warning at 8 or 9 is the threshold the NovaMX portal check also uses, because a change at a mail platform can push an office over 10.

Not measured: DKIM, because the selector does not follow reliably from DNS alone. Not measured: whether one mx term returns more than 10 address records, and whether more than two lookups come back empty. Not measured: software versions, open ports, or the contents of files. A timeout is not counted as "missing". For DMARC that count was zero.

4 DMARC policy

DMARC lives in a separate DNS record and has a policy, written as `p=`. That policy is the request to the receiver. Of the 854 domains, 68.6% have no policy that asks receivers to reject a suspicious message. That outcome has three parts.

No record (216 domains, 25.3%). There is no DMARC instruction. Receivers decide for themselves what to do with a message that fails the sender check.

p=none (369 domains, 43.2%). The record exists. The policy asks receivers to deliver the message anyway, even when the check fails. This is a monitoring stance, and only useful if a report address is present. Without that address nothing comes back. The next section covers that.

Enforcing (268 domains, 31.4%). Of those, `p=quarantine` is on 149 domains (17.4%) and `p=reject` on 119 (13.9%). Quarantine asks the receiver to treat the message as suspicious, usually by setting it aside. Reject asks the receiver to refuse it. One record was invalid.

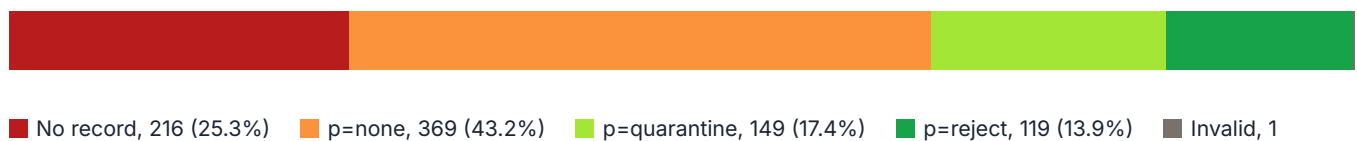


Figure 1. DMARC policy on 854 unique domains.

Most domains do publish a DMARC record. In the majority of cases that record still does not ask for action.

5 RUA and RUF

A DMARC record can contain two kinds of report address. `rva` is the address for aggregate reports: which systems tried to send mail using the domain. `ruf` is the address for failure reports about individual messages. Only a filled-in mailto address counts. A size limit after the address still counts as a request.

Among the 638 domains with a DMARC record, 37.9% ask for an aggregate report and 16.5% ask for a failure report. In this measurement, `ruf` never appears without `rva`.

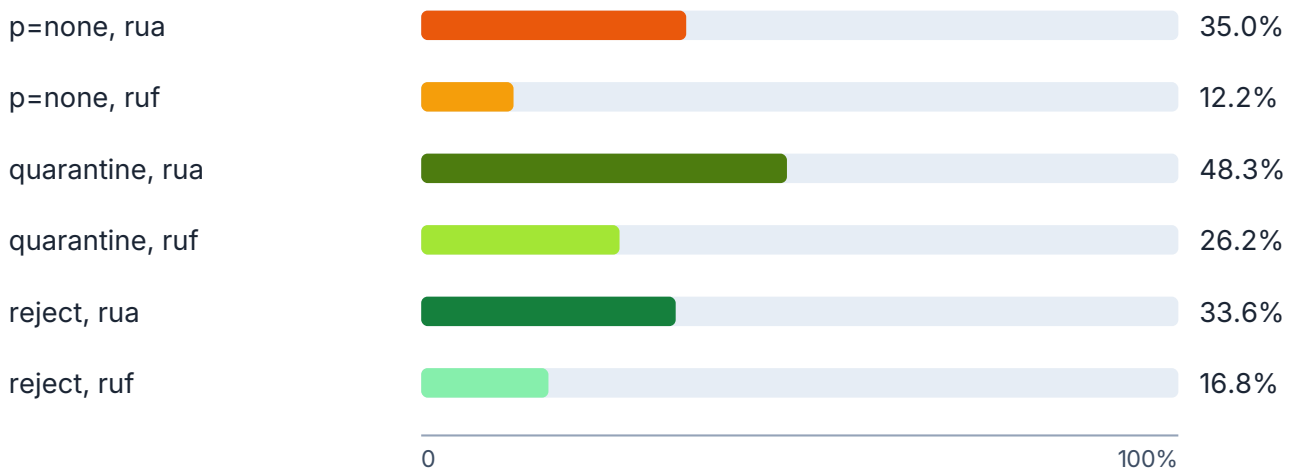


Figure 2. Share of domains with a mailto address for rua or ruf, by policy.

Policy	Domains	rua	ruf	Both	Neither
p=none	369	35.0%	12.2%	12.2%	65.0%
p=quarantine	149	48.3%	26.2%	26.2%	51.7%
p=reject	119	33.6%	16.8%	16.8%	66.4%

Table 1. Report requests among domains that publish that policy. Percentages are of the row.

At p=none, 65.0% also request no report at all. The record is published and gives the office no information.

p=quarantine requests reports most often (48.3% have rua). At p=reject, 66.4% have no report address: those offices ask receivers to refuse, and do not see what happens next.

6 SPF

SPF is the list of systems allowed to send mail for the domain. The list usually ends with a closer. -all means: anyone not on the list may not send. ~all means: anyone not on the list is suspicious, but many receivers still deliver that message. Without a closer, or with ?all or +all, the list barely restricts anyone. Two SPF records at once make the check invalid: receivers may ignore the result.

24 domains (2.8%) have no SPF record. 533 (62.4%) end in -all. 280 (32.8%) end in ~all. 11 records have no all term. 3 domains publish two SPF records. 3 records close with ?all or +all.

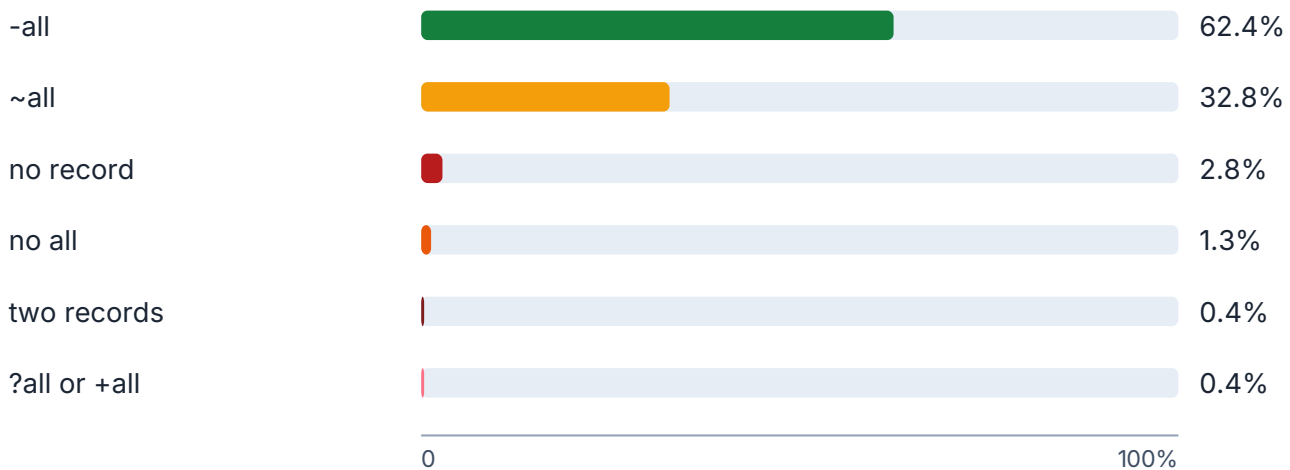


Figure 3. SPF on 854 unique domains.

SPF says who may send. Without enforcing DMARC, a receiver remains free to deliver a message that fails that test. A strict SPF record and a DMARC policy of p=none are two separate outcomes.

7 SPF lookups and flattening

An SPF list often points on to other DNS names, for example the office's sending service. Each such reference is a lookup, including when that name points further. Receivers may stop at 10 lookups. The check can then count as failed, even when the list is right in substance. Flattening replaces those references with the underlying addresses, so the list stays under that limit.

Of the 827 domains with exactly one SPF record, 61 (7.4%) are at 10 or more lookups. There, SPF can already be a permanent error for receivers. Another 91 (11.0%) are at 8 or 9: one extra sending service can push them over the limit. 673 (81.4%) stay at 7 or below. The median is 4. The highest fully counted total is 15. For 2 domains the chain broke before the count was complete.

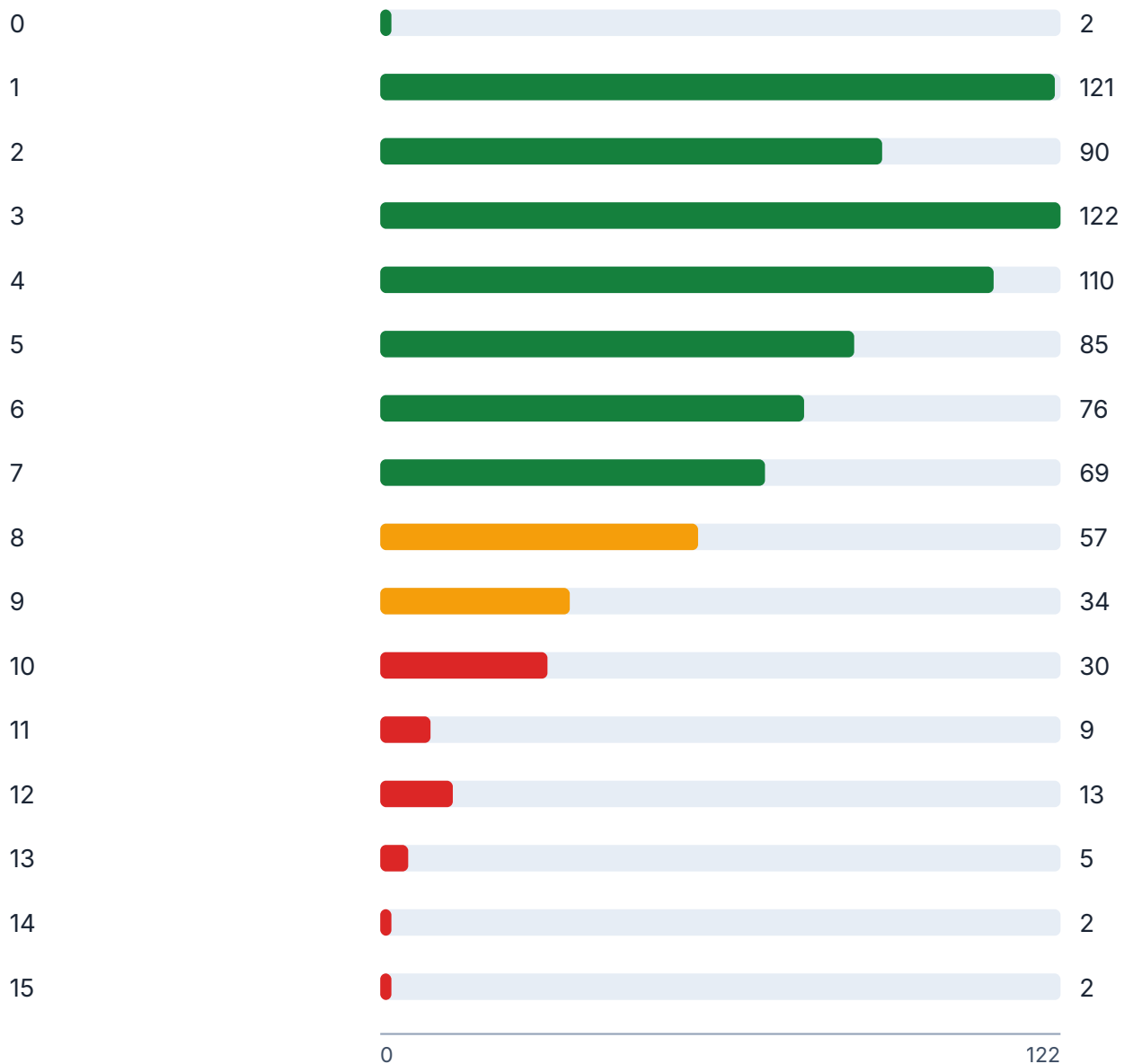


Figure 4. Number of domains per lookup count, among domains with one SPF record. Green is under 8, amber is 8 or 9, red is 10 or more.

Lookups	Domains
0	2
1	121
2	90
3	122
4	110
5	85
6	76
7	69
8	57
9	34
10	30
11	9
12	13
13	5
14	2
15	2

Table 2. Number of domains per lookup count, among domains with one SPF record.

Flattening applies to a minority of domains. It does not explain the DMARC difference. An office with 4 lookups and $p=none$ does not have a lookup problem. The policy is still set to monitor, or there is no monitoring, if rua is missing.

The 3 duplicate SPF records and the 24 missing records sit outside these 827. Flattening does not repair a second record. Those two records have to become one record first.

8 DNSSEC, HTTPS and transport

A DS record is present at the parent for 57.8% of domains (494 of 854). DNSSEC delegation is therefore more common than enforcing DMARC. A DS record is not proof that the signatures in the zone also validate.

841 domains (98.5%) have an MX record. The office website is a different surface: 805 of the 854 sites (94.3%) offered a valid certificate. 32 had a certificate that failed verification, 15 were not reachable on HTTPS, and 2 failed in the TLS handshake. Of the sites with a valid certificate, 26.3% sent HSTS.

MTA-STTS, the agreement that delivery to the domain should use TLS, was present on 3 domains (0.4%). TLS-RPT was present on 6 (0.7%). Those are transport agreements for inbound mail, not a substitute for DMARC.

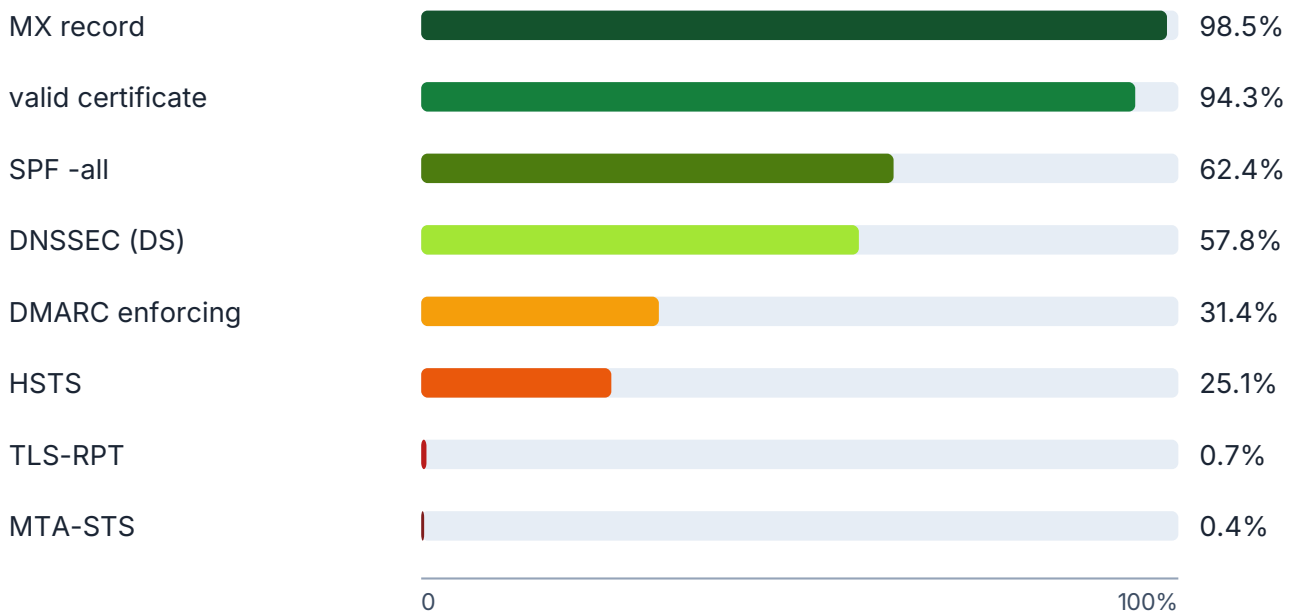


Figure 5. Share of domains per check. HSTS, SPF, DNSSEC, MX, the certificate and DMARC use 854 domains. TLS-RPT uses 851, MTA-STS 852.

9 Regions

Province follows from the office postcode. The percentages below are office-weighted. An asterisk means fewer than 40 offices; that difference is too thin for a hard comparison. Flevoland has 15 offices with an own domain. A zero share of p=reject says little there, because the group is small.

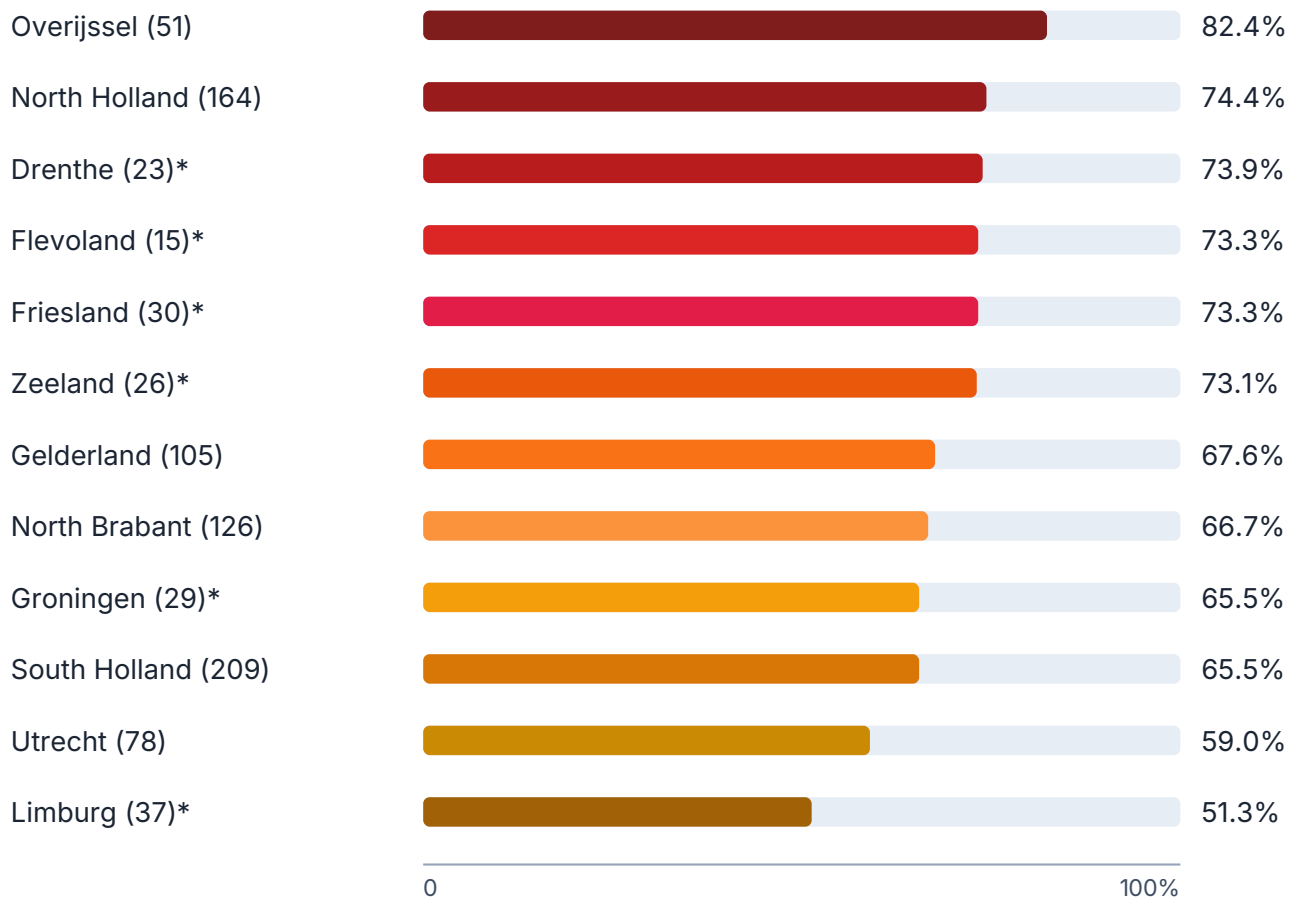


Figure 6. Share of offices without enforcing DMARC (p=none plus no record), by province. Higher means a larger share does not ask receivers to reject or quarantine.

Province	Offices	reject	quarantine	p=none	no record	no enforcement	DNSSEC	SPF - all
Overijssel	51	5.9%	11.8%	47.1%	35.3%	82.4%	72.5%	66.7%
North Holland	164	10.4%	15.2%	48.8%	25.6%	74.4%	59.8%	69.5%
Drenthe*	23	8.7%	17.4%	52.2%	21.7%	73.9%	34.8%	52.2%
Flevoland*	15	0.0%	26.7%	60.0%	13.3%	73.3%	66.7%	80.0%
Friesland*	30	16.7%	10.0%	53.3%	20.0%	73.3%	53.3%	43.3%
Zeeland*	26	11.5%	15.4%	34.6%	38.5%	73.1%	53.8%	50.0%
Gelderland	105	14.3%	18.1%	41.9%	25.7%	67.6%	65.7%	65.7%
North Brabant	126	18.3%	15.1%	36.5%	30.2%	66.7%	50.8%	63.5%
Groningen*	29	20.7%	13.8%	41.4%	24.1%	65.5%	51.7%	58.6%
South Holland	209	12.9%	21.1%	41.6%	23.9%	65.5%	56.9%	57.9%
Utrecht	78	19.2%	21.8%	38.5%	20.5%	59.0%	57.7%	64.1%
Limburg*	37	21.6%	27.0%	37.8%	13.5%	51.3%	54.1%	43.2%

Table 3. Office-weighted percentages. No enforcement is the sum of the rounded shares for p=none and no record. An asterisk: fewer than 40 offices.

Region	Offices	reject	quarantine	p=none	no record	DNSSEC
North	82	15.9%	13.4%	48.8%	22.0%	47.6%
East	171	10.5%	17.0%	45.0%	27.5%	67.8%
West	451	13.1%	19.1%	43.7%	23.9%	58.1%
South	189	18.0%	17.5%	36.5%	28.0%	51.9%

Table 4. Country regions. North is Groningen, Friesland and Drenthe. East is Overijssel, Flevoland and Gelderland. West is Utrecht, North Holland and South Holland. South is Zeeland, North Brabant and Limburg.

Among provinces with at least 50 offices, Overijssel has the lowest share of p=reject (5.9%) and the highest share with no DMARC record (35.3%). DNSSEC there is the highest, at 72.5%. Utrecht combines a higher share of p=reject (19.2%) with the lowest share of missing records among the larger provinces. North Brabant more often has no record (30.2%) and uses p=reject more often than the Randstad provinces.

Across the four regions, p=reject sits between 10.5% (East, 171 offices) and 18.0% (South, 189). West, with 451 offices, is at 13.1% and is closest to the national picture. The regional differences are smaller than the national difference between SPF ending in -all and enforcing DMARC.

10 What this means for an office

The figures describe published records. They do not show that a fake message was sent. The risk is what a receiving mail server does if such a message does arrive, and what the office itself does not see. For an administration office that is usually an invoice or a payment request that looks like the firm's own.

No DMARC, or p=none

Without a DMARC record, the receiver has no instruction. At p=none the instruction is: deliver the message, even when the sender check fails. In both cases a message that looks like the office's mail can land in the inbox. That applied to 68.6% of domains. The domain is then not asking receivers to stop it.

p=none without a report address

A p=none policy is only a way to watch if rua is filled in. Without that address the office does not see which systems try to send mail using the domain. That applies to 65.0% of the none records. The record is published, and nothing comes back.

An SPF list that does not enforce

If SPF is missing, or the list ends in ~all, ?all or +all, there is no strict boundary on who may send. ~all marks an unknown sender as suspicious, but many receivers still deliver the message. Two SPF records make the check invalid, so receivers may ignore the result. A list that ends in -all does not stop a fake message by itself either. Without DMARC set to quarantine or reject, the receiver remains free to deliver a message that misses the list.

Too many SPF lookups

At 10 or more lookups, a receiver may treat the SPF check as failed. Real mail from the office, such as an invoice, can then count as an error. At 8 or 9 lookups, one extra sending service is enough to cross that line. That is a different risk from a missing DMARC policy: the office's own mail can break while the list is still published. In this count, 7.4% of domains with one SPF record are at 10 or more, and 11.0% are at 8 or 9.

Reject without reports

p=reject asks receivers to refuse a failing message. Without rua, the office does not see which of its own systems are refused because of that, and does not see who keeps trying. Enforcing and watching are two separate choices. Of the reject records, 66.4% have no report address.

DNSSEC, the website and transport

Without a DS record at the parent, the DNS answers, including SPF and DMARC, are easier to forge in transit. A DS record does not prove that the signatures in the zone also validate. An invalid certificate, or the absence of HSTS, affects the website a client visits, not the invoice mail. Without MTA-STS the domain publishes no requirement that mail to the office be delivered encrypted. That concerns mail coming in. In this count it is rare, and it does not replace DMARC.

11 Conclusions

1. The largest difference is in DMARC policy. 68.6% of domains do not ask receivers to block or quarantine fake mail.
2. SPF is rarely missing. 62.4% end in -all and 2.8% have no SPF.
3. A DMARC record of p=none without rua is not monitoring. That applies to 65.0% of the none records.
4. Reports and enforcement do not move together. Quarantine asks for rua more often than reject. A reject without rua enforces, without the office receiving reports.
5. SPF flattening is required for 61 domains that meet or pass the lookup limit, and worth planning for another 91 at 8 or 9. It does not explain the DMARC figures.
6. DNSSEC delegation (57.8%) and valid website certificates (94.3%) are more common than enforcing DMARC. HSTS and MTA-STS are not.
7. Region explains some of the spread, especially Overijssel compared with Utrecht where the counts are large enough. It does not change the national conclusion.

12 What this measurement does not say

This is not a judgment of an office's professional work and not a penetration test. DKIM was not measured, so an office can send signed mail while its DMARC policy is still none. A valid website certificate says nothing about the mail flow. A missing DMARC record does not mean a fraud happened this week. It means receivers have not been given an instruction by the domain.

The list of individual domains is not published. An office can check its own domain with the [free mail check](#). Background on the terms is in the guides on [DMARC](#), [RUA](#) and [the ten SPF lookups](#).

About NovaMX

NovaMX B.V. is based in Beverwijk and publishes this research under its own name. MailControl, the product for DMARC reports, managed DMARC policy and SPF flattening, is on the [mail security page](#). Rates are on the [pricing page](#). Those pages are not an annex to the figures.

Questions about the method: contact@novamx.eu.