harbourline.example

Email Security Check | 13 October 2026, 06:40 UTC

C

Overall grading 60/100

Anyone can send email that looks like it came from this domain and receivers are asked to deliver it anyway.

Grade driven by: DMARC is published but set to take no action

1	2	1
HIGH	MEDIUM	LOW

About this check

What we checked

We read the public DNS records that govern who is allowed to send email using this domain name — SPF, DKIM and DMARC — along with the mail servers it publishes. Nothing was sent and no mailbox was touched.

Why it matters

These three records are what stops anyone on the internet putting your domain in the From line of an email. Without them, a message that appears to come from your company can be delivered to your customers, your staff or your suppliers, and nothing in the message will look wrong to them. This is how most invoice fraud begins.

How to read the grade

Each record contributes points, weighted by how much protection it actually provides — a DMARC policy set to take no action scores far below one that rejects. The grade explanation names the heaviest deductions.

Subdomains: why a name that sends no mail still needs these records

Sending and receiving are separate things, and this is the point most often missed. A name with no mail server can still be put in the From line of a message: somebody can send as ceo@www.example.com to a supplier, a customer or your own staff, even though nothing at www.example.com could ever receive a reply. Whether that message is delivered is decided entirely by the RECIPIENT's mail server, using the records published here — so a hostname that receives no mail is still worth protecting, and is often the easier one to forge precisely because nobody is watching it.

A wildcard DNS record is only used for names that do not already exist in your zone. Any name your zone already knows about blocks it — not just a host with an address record, but any name carrying any record at all, and even a name that exists only because something below it does. A lookup for such a name returns nothing rather than the wildcard. So a wildcard protects the names nobody is trying to forge and misses www, mail and every other host you actually run.

SPF does not inherit. It is checked against the envelope sender — the address the receiving server is given during delivery, not the From line the reader sees — so www.example.com gets no protection from the record on example.com. Publish v=spf1 -all on every hostname that never sends mail. A wildcard TXT record is worth adding as well, but it only closes names that do not exist.

DMARC does inherit, and it is the record that covers everything. A receiver that finds no policy on a subdomain falls back to the one on your main domain and applies its sp= value, or its p= value when sp= is absent. One policy at the top protects every subdomain, so no wildcard is needed — set sp=reject explicitly so the rule is stated rather than inherited by default.

DKIM does not work this way at all. Keys are published per selector, and the signer chooses both the selector and the domain. A wildcard under _domainkey is publishable and would answer for every selector, which is worse than useless: it offers one key for selectors you have never signed with.

MX follows the same rule as SPF. An MX record pointing at a single dot declares that a name receives no mail, and it has to be published on each name; a wildcard MX only covers names that do not exist.

Findings (4)

#	Finding	Risk
1	DMARC Policy Not Enforced — Impersonation is being watched, not blocked	HIGH
2	SPF Soft Fail — Your SPF record does not ask for impersonated mail to be refused	MEDIUM
3	Missing MTA-STS — Mail to this domain can be delivered unencrypted	MEDIUM
4	Missing TLS-RPT — No reports when encrypted delivery fails	LOW

HIGH 1. DMARC Policy Not Enforced — Impersonation is being watched, not blocked

CWE-290

Your DMARC policy is set to "none". That collects reports about who is sending as your domain, but asks receivers to deliver the mail anyway — including mail from people impersonating you. It is the first stage of a rollout, not the finished article.

Inferred - read from published records or response headers, not tested directly.

What to do

Once the DMARC reports show only senders you recognise, change p=none to p=quarantine, then to p=reject. Each step is a one-line DNS change and can be reversed instantly.

MEDIUM 2. SPF Soft Fail — Your SPF record does not ask for impersonated mail to be refused

CWE-290

SPF is published, but it ends in ~all, which asks receivers to accept a message from an unlisted server and only mark it.

Inferred - read from published records or response headers, not tested directly.

What to do

End the record with -all once you are sure every legitimate sender is listed.

MEDIUM 3. Missing MTA-STS — Mail to this domain can be delivered unencrypted

CWE-319

MTA-STS is not set up. It is what tells other mail servers that they must use encryption when delivering to you, and must refuse to deliver if encryption cannot be negotiated. Without it, an attacker positioned between two mail servers can strip the encryption and read the messages in transit.

Inferred - read from published records or response headers, not tested directly.

What to do

Publish an MTA-STS policy: a TXT record at _mta-sts.harbourline.example and a policy file at https://mta-sts.harbourline.example/.well-known/mta-sts.txt. Start in testing mode, then switch to enforce.

LOW

4. Missing TLS-RPT — No reports when encrypted delivery fails

CWE-16

TLS-RPT is not set up, so if another provider cannot deliver mail to you securely, nobody is told. Delivery problems of this kind are otherwise invisible until a customer says they never received something.

Inferred - read from published records or response headers, not tested directly.

What to do

Add a TXT record at _smtp._tls.harbourline.example — "v=TLSRPTv1; rua=mailto:tls@harbourline.example".

Email security detail

What each published record says, and the state we found it in. "Not checked" means we could not establish an answer — it is not a pass. The raw lookups behind all of it follow this section.

Mail servers

2 mail servers published for harbourline.example, in the order sending servers should try them.

Pri 10	**mx1.mail.example.net** 198.51.100.10
Pri 20	**mx2.mail.example.net** 198.51.100.11

Published records

SPF, DKIM and DMARC are what stop someone sending email in this domain's name. MTA-STS and TLS-RPT protect mail in transit; BIMI is branding and carries no security weight.

WARN **SPF**

ends in ~all (accept anything else but mark it) · 2 of the 10 permitted DNS lookups used · authorises 1 other sender

```
v=spf1 include:spf.mail.example.net ~all
```

- it ends in ~all, which asks receivers to accept a message from an unlisted server and only mark it.

PASS **DKIM**

signing keys found: selector1 (rsa 2048-bit) · 6 common selector names tried; selectors cannot be listed from DNS, so a key under a name we did not guess would not be found

WARN **DMARC**

policy p=none (forged mail is delivered normally; this only monitors) · aggregate reports requested · alignment adkim=r aspf=r

```
v=DMARC1; p=none; rua=mailto:dmarc@harbourline.example
```

NOT SET **MTA-STS**

NOT SET **TLS-RPT**

NOT SET **BIMI**

Technical addendum: DNS responses

Exactly what was asked of DNS and what came back — the evidence behind every check in this report. Your DNS administrator can verify each record here without taking our word for it.

MX harbourline.example
```
10 mx1.mail.example.net
20 mx2.mail.example.net
```

TXT harbourline.example
```
v=spf1 include:spf.mail.example.net ~all
```

TXT _dmarc.harbourline.example
```
v=DMARC1; p=none; rua=mailto:dmarc@harbourline.example
```

TXT selector1._domainkey.harbourline.example
```
v=DKIM1; k=rsa; p=MIIBIjANBg...
```

Reference: what these standards mean

SPF — Sender Policy Framework

SPF is a DNS record listing the servers allowed to send mail for your domain. A receiving server checks it against the sending address; an unlisted sender fails, and the message may be rejected or filtered. The whole check may use at most 10 DNS lookups — each include:, a, mx, ptr and exists: costs one, and so do the providers you include. Exceed the limit and the record fails permanently, at which point most receivers treat the domain as having no SPF at all.

DKIM — DomainKeys Identified Mail

DKIM adds a cryptographic signature to each message. Receivers fetch the public key from DNS at selector._domainkey.yourdomain and verify it. A pass proves the message was not altered in transit and that the sending domain takes responsibility for it. There is no way to discover which selector a domain uses — DNS will confirm whether a specific name exists but will not list them — so an automated check can only try the common names, and a miss is never proof that DKIM is absent.

DMARC — Domain-based Message Authentication

DMARC tells receivers how to handle mail that fails SPF and DKIM. p=none only collects reports; p=quarantine sends forgeries to spam; p=reject refuses them outright. The usual path is none, then quarantine, then reject, reading the reports at each step. The rua= address is what makes those reports exist; enforcement without reporting is acting with the lights off.

MTA-STS — Strict Transport Security

MTA-STS requires TLS, with valid certificates, for mail delivered to you. It has two halves: a DNS TXT record at _mta-sts.yourdomain, and a policy file served over HTTPS at https://mta-sts.yourdomain/.well-known/mta-sts.txt. Both must work. A record advertising a policy that cannot be fetched is worse than publishing neither, because senders that cached it keep enforcing it.

TLS-RPT — SMTP TLS Reporting

TLS-RPT is a DNS record telling receiving servers where to send reports about your domain's TLS delivery results. It surfaces certificate problems, downgrade attacks and failed handshakes without exposing message content. Publish it at _smtp._tls.yourdomain, alongside MTA-STS.

BIMI — Brand Indicators for Message Identification

BIMI lets participating mailbox providers show your logo beside authenticated mail. It only works once DMARC is enforced (quarantine or reject), and some providers also require a Verified Mark Certificate. It does not change delivery — fix the authentication underneath before adding it.

Report generated 17 October 2026, 19:36 UTC. Scan reference 59a718b8-8203-4a88-851c-a2df51d0a90d.