

SAMPLE REPORT · FICTIONAL BUSINESS

SPF · DKIM · DMARC · MTA-STS · DNSSEC

Email Security Report

harborpointlogistics.example

Harbor Point Logistics · Prepared for Jordan Rivera
Scanned October 22, 2026 at 9:30 AM EDT
jordan@harborpointlogistics.example

Report ID MVJKVW00

D

SPOOF RISK HIGH

SCORE 56 / 100

CONTENTS

01	Summary	2
02	Fix plan	3
03	Check details	5
04	How the grade works	7
05	Next steps, sources & disclaimer	7

Provided by All Business Technologies. Not affiliated with Google, Yahoo, Microsoft or any email provider.

01 · SUMMARY

Where your domain stands

Live check of the public DNS records that control who can send email as harborpointlogistics.example, run October 22, 2026. 7 graded checks plus BIMI as an optional extra.



At a glance

Weak. Your domain is easy to spoof.

● Mail servers	PASS
● SPF	PASS
● DMARC	WARNING
● DKIM	WARNING
● MTA-STS	WARNING
● TLS reporting	WARNING
● DNSSEC	WARNING
● BIMI	OPTIONAL

Your mail setup

Mail provider	Microsoft 365
Senders listed in SPF	Microsoft 365, Mailchimp, SendGrid, Salesforce
DMARC policy	p=none
SPF DNS lookups	6 of 10
DNS queries	48 via Google Public DNS

02 · FIX PLAN

5 things to fix

Ordered by how much each one reduces spoofing risk. Give these records to whoever manages your DNS. Change one thing at a time and watch your DMARC reports.

01 DMARC (what to do with fakes)

HIGH

p=none: monitoring only. Spoofed mail still gets delivered.

DMARC tells receivers what to do with mail that fakes your domain, and sends you reports on who is sending as you.

Next step: start quarantining failures

```
Host: _dmarc.harborpointlogistics.example
Type: TXT
Value: v=DMARC1; p=quarantine; pct=100; rua=mailto:it@harborpointlogistics.example; fo=1
```

- Before switching, confirm in your DMARC reports that every real sender passes SPF or DKIM.
- After a few clean weeks on quarantine, move to p=reject.

02 DKIM (tamper-proof signature)

MEDIUM

Found 2 keys, but s1 uses a 1024-bit key.

1024-bit RSA keys are considered weak today; 2048-bit is the common recommendation.

- Rotate to a 2048-bit key in your provider's DKIM settings, publish the new record, then retire the old selector.

03 MTA-STS (force encrypted delivery)

HARDENING

Not set up.

MTA-STS (RFC 8461) tells other mail servers to only deliver to you over verified, encrypted TLS, which blocks downgrade and interception attacks on mail in transit.

1. Publish this TXT record

```
Host: _mta-sts.harborpointlogistics.example
Type: TXT
Value: v=STSV1; id=2026102201
```

2. Serve this file at <https://mta-sts.harborpointlogistics.example/.well-known/mta-sts.txt>

```
version: STSV1
mode: testing
mx: harborpointlogistics-example.mail.protection.outlook.com
max_age: 604800
```

- Start in mode: testing with TLS reporting on, then switch to mode: enforce once reports are clean.
- Change the id= value whenever you change the policy file.

04 TLS reporting (TLS-RPT)

HARDENING

Not set up.

TLS-RPT (RFC 8460) sends you daily reports when other servers have trouble delivering to you securely. Pair it with MTA-STS.

Add this TXT record

```
Host: _smtp._tls.harborpointlogistics.example
Type: TXT
Value: v=TLSRPTv1; rua=mailto:tls-reports@harborpointlogistics.example
```

05 DNSSEC (signed DNS)

HARDENING

Not signed.

DNSSEC stops attackers from forging DNS answers, including your MX, SPF and DMARC records. Most registrars and DNS hosts can turn it on with one switch.

- Turn on DNSSEC at your DNS host (for example Cloudflare: DNS > Settings > DNSSEC), then add the DS record at your registrar if it is not automatic.

03 · CHECK DETAILS

Every check, explained

What each record does and exactly what we found in public DNS.

● Mail servers (MX)

PASS · 10/10 pts

1 mail server · Microsoft 365

MX records tell the world which servers accept email for your domain.

```
MX 10 harborpointlogistics-example.mail.protection.outlook.com
```

● SPF (who may send as you)

PASS · 22/25 pts

Valid, ends in ~all (soft fail) · 6 of 10 lookups

SPF lists the servers allowed to send email as your domain.

```
harborpointlogistics.example TXT "v=spf1 include:spf.protection.outlook.com include:servers.mcsv.net include:sendgrid.net include:_spf.salesforce.com ~all"
DNS lookups: 6 of 10
```

● DMARC (what to do with fakes)

WARNING · 12/35 pts

p=none: monitoring only. Spoofed mail still gets delivered.

DMARC tells receivers what to do with mail that fakes your domain, and sends you reports on who is sending as you.

```
_dmarc.harborpointlogistics.example TXT "v=DMARC1; p=none; rua=mailto:it@harborpointlogistics.example"
```

● DKIM (tamper-proof signature)

WARNING · 10/15 pts

Found 2 keys, but s1 uses a 1024-bit key.

1024-bit RSA keys are considered weak today; 2048-bit is the common recommendation.

```
selector1._domainkey.harborpointlogistics.example: 2048-bit RSA
s1._domainkey.harborpointlogistics.example: 1024-bit RSA
```

● MTA-STS (force encrypted delivery)**WARNING · 0/5 pts**

Not set up.

MTA-STS (RFC 8461) tells other mail servers to only deliver to you over verified, encrypted TLS, which blocks downgrade and interception attacks on mail in transit.

```
_mta-sts.harborpointlogistics.example TXT none  
mta-sts.harborpointlogistics.example does not resolve
```

● TLS reporting (TLS-RPT)**WARNING · 0/4 pts**

Not set up.

TLS-RPT (RFC 8460) sends you daily reports when other servers have trouble delivering to you securely. Pair it with MTA-STS.

```
_smtp._tls.harborpointlogistics.example TXT none
```

● DNSSEC (signed DNS)**WARNING · 0/3 pts**

Not signed.

DNSSEC stops attackers from forging DNS answers, including your MX, SPF and DMARC records. Most registrars and DNS hosts can turn it on with one switch.

```
DNSSEC validated: no  
Name servers: ns1.example-dns.net, ns2.example-dns.net
```

● BIMI (brand logo in inbox)**OPTIONAL**

Optional. Needs DMARC at quarantine or reject first.

BIMI lets supporting inboxes show your logo next to mail that passes DMARC. Gmail and Apple Mail also require a Verified Mark Certificate or Common Mark Certificate. It is a branding bonus, not a security control, so it does not affect your grade.

```
default._bimi.harborpointlogistics.example TXT none
```

04 · HOW THE GRADE WORKS

How your grade works

- Points: DMARC 35, SPF 25, DKIM 15, MX 10, MTA-STS 5, TLS reporting 4, DNSSEC 3. Partial setups earn partial points; checks that do not apply are left out.
- Caps: if SPF or DMARC is missing or broken, the grade cannot be above D. If DMARC is p=none, it cannot be above C.
- Grades: A 90-100, B 75-89, C 60-74, D 45-59, F below 45. A+ adds a published BIMl logo. ABT set these weights and bands; no standards body defines them.
- Limits: DKIM keys cannot be listed from DNS, so common selector names were probed. Results are a snapshot of public DNS at scan time.

Want a second set of eyes on this?

ABT has managed IT and cybersecurity for businesses since 2003. We'll walk through this report with you and help you roll out the fixes safely, without breaking your mail.

[Book a free consultation](#)[Call \(508\) 586-1000](#)

Sources

1. FBI Internet Crime Complaint Center, 2024 Internet Crime Report (Business Email Compromise losses).
https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf
2. Google, Email sender guidelines.
<https://support.google.com/a/answer/81126>
3. Yahoo, Sender best practices.
<https://senders.yahooinc.com/best-practices/>
4. Microsoft, Outlook's new requirements for high-volume senders.
<https://techcommunity.microsoft.com/blog/microsoftdefenderforoffice365blog/strengthening-email-ecosystem-outlook%E2%80%99s-new-requirements>
5. CISA, Binding Operational Directive 18-01: Enhance Email and Web Security.
<https://www.cisa.gov/news-events/directives/bod-18-01-enhance-email-and-web-security>
6. RFC 7208, Sender Policy Framework (SPF).
<https://www.rfc-editor.org/rfc/rfc7208>
7. RFC 6376, DomainKeys Identified Mail (DKIM) Signatures.
<https://www.rfc-editor.org/rfc/rfc6376>
8. RFC 7489, Domain-based Message Authentication, Reporting, and Conformance (DMARC).
<https://www.rfc-editor.org/rfc/rfc7489>
9. RFC 8461, SMTP MTA Strict Transport Security (MTA-STS).
<https://www.rfc-editor.org/rfc/rfc8461>

10. RFC 8460, SMTP TLS Reporting.
<https://www.rfc-editor.org/rfc/rfc8460>
11. RFC 7505, A "Null MX" No Service Resource Record.
<https://www.rfc-editor.org/rfc/rfc7505>
12. BIM! Group, Brand Indicators for Message Identification.
<https://bimigroup.org/>

Informational only. Results come from public DNS at the moment of the scan and cannot see inside your mail system. DKIM keys under custom selector names may not be detected. Test DNS changes carefully: a wrong SPF or DMARC record can stop legitimate mail. This report is not a substitute for a professional security assessment.

Provided by All Business Technologies. Not affiliated with Google, Yahoo, Microsoft or any email provider.