

Stop people sending email as you

Five DNS records decide whether someone can send convincing email in your name. What each one does, what it looks like, and where it usually goes wrong.

01 SPF Which servers may send mail as you? Free	02 DKIM Was the message signed and left unchanged? Free	03 DMARC What happens when those checks fail? Free	04 MTA-STS Is mail to you encrypted in transit? Free + HTTPS site	05 BIMI Can inboxes show your logo? ≈ US\$750-1,500/yr
--	--	---	--	---

THE RECORDS

01 SPF

TXT at
example.com

```
v=spf1 include:spf.protection.outlook.com include:servers.mcsv.net -all
```

- One SPF record per domain. Two records make both invalid.
- Ten DNS lookups at most, and every include: counts. End with -all or ~all, never +all.

02 DKIM

TXT or CNAME at
selector._domainkey.
example.com

```
si._domainkey.example.com TXT "v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAO..."
```

- Turn it on for every service that sends as you: CRM, newsletter, invoicing, ticketing, not only your mailbox.
- Use 2048-bit keys and publish the record exactly as the provider gives it.

03 DMARC

TXT at
_dmarc.example.com

```
v=DMARC1; p=none; rua=mailto:dmarc@example.com ← start: monitor
v=DMARC1; p=reject; rua=mailto:dmarc@example.com ← goal: block
```

- p=none only watches. Alignment matters: the domain that passes SPF or DKIM must match the From domain.
- Google and Yahoo (Feb. 2024) and Microsoft Outlook.com (May 2025) require DMARC from senders of 5,000+ messages a day.

04 MTA-STS

TXT at
_mta-sts.example.com
policy at
https://mta-sts.
example.com/.well-
known/mta-sts.txt

```
_mta-sts.example.com TXT "v=STSV1; id=20261013"
mta-sts.txt: version: STSV1 · mode: enforce · max_age: 604800
mx: *.mail.protection.outlook.com
_smtp._tls.example.com TXT "v=TLSRPTv1; rua=mailto:tlsrpt@example.com"
```

- Start with mode: testing and read the TLS reports before enforcing.
- Change the id whenever you edit the policy, and keep the mx lines in sync with your MX records.

05 BIMI

TXT at
default._bimi.
example.com

```
v=BIMI1; l=https://example.com/logo.svg; a=https://example.com/vmc.pem
```

- Needs DMARC at p=quarantine or p=reject, and a logo in SVG Tiny PS format.
- Gmail and Apple Mail need a mark certificate: a VMC (registered trademark, adds Gmail's blue checkmark) or, for Gmail, a CMC (logo in use for 12+ months).

ROLL OUT DMARC WITHOUT BREAKING YOUR MAIL

1

List your senders

Mailbox, CRM, newsletter, invoicing, web forms, scanners

2

SPF + DKIM

Publish SPF, turn on DKIM for each sender

3

Monitor

DMARC at `p=none`, read reports for a few weeks

4

Fix failures

Until legitimate mail passes alignment

5

Enforce

Quarantine, then reject. Ramp with `pct=25` if needed

`p=none`

Monitor only. Spoofed mail still lands.

`p=quarantine`

Failing mail goes to spam.

`p=reject`

Failing mail is refused. The goal.

Domains you own but don't send from

SPF	<code>v=spf1 -all</code>
DMARC	<code>v=DMARC1; p=reject</code>
MX	<code>0 .</code> (null MX, accepts no mail)

Where to turn on DKIM

Microsoft 365	Defender portal > Email & collaboration > Policies & rules > Threat policies > Email authentication settings > DKIM
Google Workspace	Admin console > Apps > Google Workspace > Gmail > Authenticate email

Check your records

SPF	<code>dig +short TXT example.com</code>
DMARC	<code>dig +short TXT _dmarc.example.com</code>
DKIM	<code>dig +short TXT s1._domainkey.example.com</code>
MTA-STS	<code>dig +short TXT _mta-sts.example.com</code>
BIMI	<code>dig +short TXT default._bimi.example.com</code>
Windows	<code>nslookup -type=TXT _dmarc.example.com</code>

YOUR CHECKLIST

- ☐ Exactly one SPF record, under 10 lookups
- ☐ DKIM on for every service that sends as you
- ☐ DMARC reports going to a mailbox someone reads
- ☐ DMARC at `p=reject`, or a dated plan to get there
- ☐ Subdomains covered (`sp=reject` once at reject)
- ☐ MTA-STS in enforce mode, with TLS reports
- ☐ Parked domains locked down
- ☐ An owner for this when a new sending service is added

RECORDS STOP SPOOFING, NOT EVERY SCAM

- Confirm any change of payment details by calling a number you already have, never one in the email.
- Treat urgency and secrecy as warning signs, especially from executives or suppliers.
- Check the actual sender address, not the display name. Lookalike domains pass every check above.
- Report suspicious messages to IT instead of just deleting them.

TOOL WE USE **Ongoing DMARC monitoring.** Reports are hard to read by hand. We use **Mailsec** (mailsec.ca), a Canadian DMARC and domain-security platform, to monitor reports and catch new senders.

Disclosure: Mailsec is a client of Privateer Cybersecurity and may pay us a referral fee.

Want it set up for you, or a second pair of eyes on your records?

Senior help in English or French. We reply within 1–2 business days.



privateer.ca · info@privateer.ca