DVG Systems

A DVG SYSTEMS GUIDE · EDITION 2026

The Email Security Guide for Canadian SMBs

Microsoft's bulk-sender enforcement went live May 5, 2025 — following Google and Yahoo in February 2024. This is the guide your IT provider should have given you months ago.

www.dvgsystems.com · (807) 700-0061 v2026.04

> ### If your emails have been landing in junk, this is why
>
> Starting **May 5, 2025**, Microsoft began rejecting messages from high-volume senders (5,000+ emails/day to `outlook.com`, `hotmail.com`, `live.com`) that don't publish SPF, DKIM, and DMARC. Rejected mail comes back with `550 5.7.15 Access denied`. Google and Yahoo did the same thing in February 2024.
>
> Even if you're well below the 5,000/day threshold, you're still being judged. Every business inbox that uses Microsoft 365, Gmail, or Yahoo-based filtering reads the same signals. Missing one of these three records makes the difference between "arrived in inbox" and "never seen."
>
> This guide shows you what to check, how to fix it, and how to verify you stay passing.

The three records, explained in plain English

Record	What it does	Published where
SPF Sender Policy Framework	Lists the servers authorised to send mail using your domain.	DNS TXT at the root of your domain
DKIM DomainKeys Identified Mail	Cryptographic signature on every message — proves the message wasn't tampered with.	DNS TXT (or CNAME) at a selector subdomain
DMARC Domain-based Message Authentication	Tells receivers what to do with messages that fail SPF or DKIM, and where to send reports.	DNS TXT at `_dmarc.yourdomain.ca`

You need all three. Two out of three doesn't cut it in 2026.

What the records actually look like

SPF — example for a Microsoft 365 tenant

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

If you send through third parties (Mailchimp, Constant Contact, QuickBooks, SendGrid, Resend), each one needs its own `include:`. Miss one and mail from that provider fails SPF.

DKIM — for Microsoft 365

Microsoft 365 uses two CNAME records pointing into their infrastructure. Enable DKIM signing in the Microsoft 365 Defender portal under **Email & collaboration → Policies & rules → Threat policies → Email authentication settings → DKIM**.

DMARC — start here

```
v=DMARC1; p=quarantine; rua=mailto:dmarc-reports@yourdomain.ca; pct=100; adkim=r; aspf=r
```

Break-down:

- `p=quarantine` — messages failing SPF and DKIM should go to junk.
- `rua=` — where to send aggregate reports (use a mailbox you monitor, or a service like Dmarcian, Valimail, Postmark).
- `pct=100` — apply the policy to 100% of mail.
- `adkim` / `aspf` — alignment mode (relaxed is safe to start).

> **Start at `p=none` if you've never deployed DMARC before.** Monitor the aggregate reports for 2–4 weeks to confirm you're not going to break legitimate senders. Then step up to `p=quarantine`, then `p=reject`.

The 6 gotchas that catch SMBs

1. Third-party senders not in SPF

You enabled SPF, but your accountant's QuickBooks invoices still fail because QuickBooks' servers aren't in your record. Every tool that sends mail "from" your domain needs to be in the include list: QuickBooks, Mailchimp, Constant Contact, SendGrid, Resend, ServiceTitan, HubSpot, Calendly, form-relays like web3forms or Formspark.

2. Forwarding breaks SPF

If a customer forwards your message to another inbox, SPF fails at the forwarding hop. DKIM survives forwarding — which is why DKIM is mandatory in 2026, not optional.

3. Display-name spoofing

SPF/DKIM/DMARC authenticate the *domain*, not the display name. Attackers can still send mail from `john@gmail.com` with display name "John at DVG Systems" — your policy records won't block it. Train staff to check the actual address.

4. Copy-pasted DMARC records with wrong RUA mailbox

Templates floating around Reddit or AI chatbots often point `rua=` at mailboxes that don't exist. Reports bounce. You learn nothing. Use a mailbox you can actually read, or a free-tier reporting service.

5. Exposed mail servers bypassing M365 filtering

Some line-of-business apps (old CRM, vendor scanners, printers with "scan-to-email") are still configured to SMTP-relay directly to the internet. Those messages often fail SPF because they originate from your office IP, not Microsoft's. Fix by relaying through a Microsoft 365 connector or a dedicated transactional provider.

6. Multiple SPF records

DNS allows only **one** SPF TXT record per domain. If you add a second, both fail. Consolidate every sender into one `v=spf1` record.

What a failing DMARC costs you: in 2026 Microsoft reports to senders if their domain is flagged as risky. Your prospects see "This message may not be safe" banners inside Outlook. Your win-rate on cold outreach can drop 30–50% before you realise what's happening.

How to verify — 15 minutes

1. Run a free scan at `mxtoolbox.com/deliverability` with your domain. It reports SPF, DKIM, DMARC, blacklist status.
2. Send a test message to `check-auth@verifier.port25.com` — the reply tells you how the message was authenticated.
3. Send yourself a test from each line-of-business app (invoicing, booking, CRM). Look at the raw headers (Gmail: "Show original"; Outlook: "View source"). Confirm SPF = pass, DKIM = pass, DMARC = pass.
4. Inspect the `rua=` mailbox (or your DMARC reporting service). Look for surprise senders.
5. Save a screenshot of MXToolbox's green "all passed" result. Keep it with your cyber insurance evidence — it answers the email-authentication questions on the renewal form.

The 2026 ramp-up roadmap

If you're behind, here's how to catch up in under 30 days without breaking mail.

Week	Action	Output
1	Publish SPF with your primary sender only. Enable DKIM on the primary sender.	SPF + DKIM passing on primary mail flow.
1–2	Inventory every third-party sender. Add each to SPF (or use a SPF-flattening service if you're near the 10-lookup limit).	All senders listed.
2	Publish DMARC at `p=none` with RUA pointing to a monitored mailbox or reporting service.	Reports flowing in.
3	Review DMARC reports. Remediate any surprise senders (unauthorised, misconfigured).	Clean report baseline.
4	Step DMARC to `p=quarantine; pct=25`, then climb weekly to `pct=100`.	Enforced quarantine.
5–8	Step to `p=reject` once aggregate reports show zero unexpected failures for 2 consecutive weeks.	Full protection.

One-click attestation for the renewal form

When your cyber insurer or client vendor form asks about email authentication, answer with the 3 lines below and attach the MXToolbox screenshot.

SPF: Published. Hard-fail (`-all`). Includes all authorised senders; validated with MXToolbox.

DKIM: Enabled on primary sender (Microsoft 365). 2048-bit keys. Signing confirmed on outbound sample.

DMARC: Published at `p=quarantine`, escalating to `p=reject` on [target date]. Aggregate reporting to a monitored mailbox.

Sources

1. Microsoft, "Strengthening the Email Ecosystem: Outlook's New Requirements for High-Volume Senders" (May 2025) — techcommunity.microsoft.com
2. Google Workspace, "Email Sender Guidelines FAQ" — support.google.com
3. Yahoo Sender Hub — senders.yahooinc.com
4. IETF RFC 7208 (SPF), RFC 6376 (DKIM), RFC 7489 (DMARC)
5. Canadian Centre for Cyber Security, "Don't take the bait: Recognize and avoid phishing attacks" — cyber.gc.ca

Want us to run the audit and handle the DNS work?

DVG Systems runs a for any Canadian business: we pull your current SPF / DKIM / DMARC posture, produce the remediation plan, and can handle the DNS and Microsoft 365 configuration end-to-end. Most small businesses move from "failing" to "passing" inside two weeks.

TALK TO US
(807) 700-0061

EMAIL
solutions@dvgsystems.com

BOOK ONLINE
www.dvgsystems.com/contact