CASE STUDY

EMAIL AUTHENTICATION

SPF / DKIM / DMARC / routing

Email authentication hardening and audit toolkit for live domains

Production domains in active use · Read-only audit tooling + live DNS fixes · Role: builder and operator

Outcome: Domains pass SPF, DKIM, and DMARC checks; spoofed mail is rejected instead of delivered; a reusable audit script turns a manual hour of DNS checking into a 30-second pass.

The Situation

Email spoofing is the cheapest attack there is: if a domain's SPF, DKIM, and DMARC records are missing or misconfigured, anyone can send mail as that domain - and most small-organization domains are misconfigured, often silently. The records exist in DNS, the syntax is finicky, and nobody notices until something is spoofed or legitimate mail starts bouncing.

What Was Built

- **Built a read-only audit script** (PowerShell) that live-queries any domain's MX, SPF, DKIM (across common selectors), and DMARC posture and renders PASS / WARN / FAIL verdicts with plain-English explanations of each finding. (See the demo video - a real, unedited run.)
- **Fixed real misconfigurations** on production domains: SPF records missing required senders (which silently breaks mail forwarding), enforcement set too weak, missing DMARC.
- **Email routing infrastructure**: domain mail routing via Cloudflare Email Routing with correct SPF integration alongside existing Microsoft and Azure senders - three sending systems coexisting on one domain without breaking each other.

Results

- Audited domains pass authentication at major receivers; spoof attempts fail DMARC and get rejected.
- The mail-forwarding SPF misconfiguration was caught and fixed before it cost deliverability.
- The audit is now the first step of every security checkup engagement.

Stack & Methods

Stack: DNS · SPF / DKIM / DMARC · PowerShell · Cloudflare (DNS, Email Routing, API automation) · Microsoft 365 Exchange Online