Email Security: SPF, DKIM & DMARC Guide

Email remains the primary vector for cyberattacks. SPF, DKIM, and DMARC are three complementary DNS-based protocols that authenticate email senders and prevent domain spoofing. Together, they form a critical defense layer against phishing and business email compromise (BEC).

Key Points

- ✓ SPF (Sender Policy Framework) specifies which mail servers can send email for your domain
- ✓ DKIM (DomainKeys Identified Mail) cryptographically signs emails to verify they were not tampered with
- ✓ DMARC (Domain-based Message Authentication) tells receivers what to do when SPF/DKIM fail
- ✓ Start DMARC with p=none (monitor), progress to p=quarantine, then p=reject
- ✓ Review DMARC aggregate reports weekly to identify unauthorized senders
- ✓ Implement for all domains — including parked domains that should not send email
- ✓ BIMI (Brand Indicators for Message Identification) adds your logo to authenticated emails

Action Items

1. Check your domain's current SPF, DKIM, and DMARC records using MXToolbox
2. If DMARC is not set, start with a monitoring policy: v=DMARC1; p=none; rua=mailto:dmarc@yourdomain.com
3. Enroll in a DMARC reporting service to visualize aggregate reports
4. Ensure all legitimate email services are included in your SPF record
5. Set a goal to reach DMARC p=reject within 6 months

Quick Reference

DNS Record Examples:
SPF: v=spf1 include:_spf.google.com include:spf.protection.outlook.com -all
DMARC: v=DMARC1; p=reject; rua=mailto:dmarc-reports@yourdomain.com; pct=100
DMARC Policy Progression: p=none (monitor) → p=quarantine (flag) → p=reject (block)