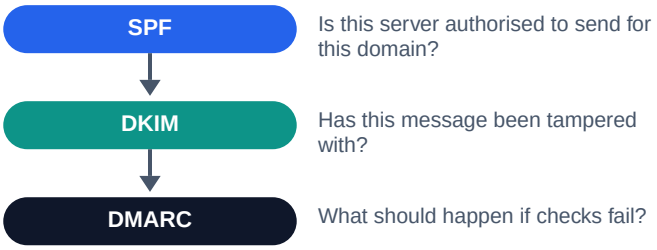
IT CLUB • EMAIL SECURITY GUIDE

CAN SOMEONE PRETEND TO EMAIL YOUR CUSTOMERS?

Understanding SPF, DKIM and DMARC

HOW EMAIL AUTHENTICATION WORKS



PASS: TRUSTED EMAIL
Authentication passes > Delivered

FAIL: SPOOFED EMAIL
Fails checks > Quarantined or Rejected

WHAT IS EMAIL SPOOFING?

Email spoofing is when a criminal sends an email that displays your company name, email address and domain in the From field — even though it was sent from a completely different server by someone with no connection to your business. Without authentication controls, there is nothing to prevent this.

THE THREE STANDARDS

SPF — Sender Policy Framework

OK: Lists the servers authorised to send email for your domain
WARNING: Does not verify the From address shown to recipients; has a 10 DNS lookup limit

DKIM — DomainKeys Identified Mail

OK: Adds a digital signature to verify the message has not been altered in transit
WARNING: Does not protect the visible From address on its own

DMARC — Domain-based Message Authentication, Reporting and Conformance

OK: Ties SPF and DKIM together; requires alignment with the From address; defines a policy; enables reporting
WARNING: Does not protect against look-alike domains or compromised accounts

Understanding DMARC

DMARC POLICY OPTIONS

p=none	**Monitor Only**	No action on failing messages — reports sent to you. START HERE.
p=quarantine	**Quarantine**	Failing messages sent to spam / junk folder. Move here after monitoring.
p=reject	**Reject**	Failing messages blocked entirely. Only set after thorough testing.

WHAT DMARC DOES NOT DO

- X Encrypt email content
- X Stop malware or viruses in attachments
- X Stop users clicking phishing links from other domains
- X Replace Microsoft Defender or endpoint security
- X Replace email filtering or anti-spam software
- X Replace multi-factor authentication (MFA)
- X Replace security awareness training
- X Replace backups
- X Protect against look-alike domains (yourcompany-support.com)
- X Prevent compromise of a genuine email account

START WITH MONITORING — NOT REJECT

1. Publish DMARC with p=none and a reporting address
2. Review aggregate reports over several weeks
3. Identify every service sending email on your behalf
4. Ensure each is in your SPF record and signing with DKIM
5. Resolve all configuration issues
6. Move to p=quarantine and monitor for unexpected impact
7. Move to p=reject only when confident all legitimate email passes

COMMON MISTAKES TO AVOID

WARNING: Multiple SPF records: A domain must have exactly one SPF record.
WARNING: Too many DNS lookups: SPF has a 10-lookup limit. Adding too many services can exceed it.
WARNING: Forgetting third-party senders: CRM, marketing, invoicing, website forms, printers and cloud services.
WARNING: Never reviewing reports: Monitoring only adds value if someone reads the reports.
WARNING: Moving to reject too quickly: Legitimate email may be blocked before configuration is complete.

DMARC is one of the best ways to stop criminals impersonating your business — but it works best when combined with good email security, monitoring and regular review.

itclub.work/
knowledge-centre