

FREE SECURITY WORKSHEET

SPF, DKIM & DMARC Email Security Worksheet

A plain-English worksheet to inventory and validate your business's email authentication.

Practical security organization guidance. Not legal, insurance, or compliance advice.

SPF, DKIM, and DMARC are email authentication records that help prove your emails are really from you — and help stop scammers from spoofing your domain. Use this worksheet to find out what's currently in place.

1 In Plain English

- **SPF** — a list of who's allowed to send email for your domain.
- **DKIM** — a digital signature that proves an email wasn't altered in transit.
- **DMARC** — the policy that tells email providers what to do if a message fails SPF or DKIM.

2 Your Domain Inventory

Domain Worksheet — Domain 1	
Domain Name	
SPF Status	☐ Present ☐ Missing ☐ Unknown
DKIM Status	☐ Present ☐ Missing ☐ Unknown
DMARC Status	☐ Present ☐ Missing ☐ Unknown
DNS Provider	
Mail Provider(s)	
Third-Party Senders	
Current DMARC Policy	☐ None ☐ Quarantine ☐ Reject ☐ Unknown
Recommended Next Step	

Domain Worksheet — Domain 2	
Domain Name	
SPF Status	☐ Present ☐ Missing ☐ Unknown
DKIM Status	☐ Present ☐ Missing ☐ Unknown
DMARC Status	☐ Present ☐ Missing ☐ Unknown
DNS Provider	
Mail Provider(s)	
Third-Party Senders	
Current DMARC Policy	☐ None ☐ Quarantine ☐ Reject ☐ Unknown
Recommended Next Step	

Need to document more than two domains? Copy this worksheet page as needed.

WHAT'S NEXT

Whether you prefer to do it yourself or work with an expert, the goal is the same: reduce your risk before it becomes a business problem.

DIY PATH

Want the expanded tracker, policy templates, vendor inventory, backup checklist, and first-24-hours incident response worksheet?

[Get the Starter Kit →](#)

DONE-WITH-YOU PATH

Prefer an expert to configure SPF, DKIM, and DMARC correctly instead of guessing?

[Book a Microsoft 365 Email Security Review →](#)