



MythsLane

IT & Cyber Security Solutions Consulting

DNS Assessment & Security Reviews

Why good DNS security matters

Good DNS security protects availability, trust, email integrity, brand reputation and operational resilience. Weak DNS controls can expose organisations to spoofing, phishing, traffic redirection, outage risk and poor internet trust posture.

Why good DNS security matters



Reduce risk

Identify and remediate misconfigurations, exposures and policy gaps to minimise attack surface.



Protect email and brand

Strengthen SPF, DKIM, DMARC and alignment to improve deliverability and protect your domain.



Improve resilience

Strengthen DNS availability, redundancy and change controls to reduce outage risk and impact.



Strengthen trust

Demonstrate DNSSEC readiness and strong governance to build internet trust.

What we assess



1 External DNS assessment

Evaluate public DNS, internet exposure, record configuration, security controls and trust services that protect your domain and users.



2 Internal DNS review

Review internal DNS architecture, forwarding, recursion, zone management and monitoring to ensure secure, reliable name resolution.



3 Protective DNS & DNS filtering

Assess DNS filtering, threat intelligence, content controls and policy enforcement to block malicious destinations and reduce risk to users and systems.

Typical checks we perform



DNS records and configurations



DNSSEC readiness



CAA, SPF, DKIM, DMARC alignment



Delegation & nameserver controls



Zone transfer exposure



Recursion exposure



Mail & TLS controls

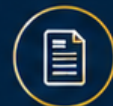


Filtering posture

How the review works



Reporting outputs



Technical Summary

Detailed findings and evidence with technical risk ratings and configuration insights.



Executive-Focused Report

Business risk and impact narrative with clear, non-technical recommendations.



Roadmap Remediation

Prioritised roadmap with quick wins, dependencies and sequencing guidance.



Follow-Up Posture Status

Repeat health checks to validate improvements and track posture over time.

Service options

Essentials



- Baseline DNS health checks across external and internal DNS
- Key misconfigurations and exposures identified
- Concise technical summary with priority findings

Ideal for a strong baseline and quick wins.

Complete



- Broader assessment of DNS controls and trust services
- Business and technical reporting for stakeholders
- Prioritised recommendations and quick-win roadmap

Ideal for organisations seeking clarity and actionable plans.

Enhanced



- Expanded scope across DNS, filtering and governance
- Remediation roadmap with dependencies and sequencing
- Follow-up posture review and advisory support

Ideal for comprehensive assurance and ongoing improvement.



Why MythsLane

MythsLane consultants bring extensive experience across DNS, internet trust, email security and cyber resilience. We combine technical depth with a business-focused approach to deliver practical recommendations that reduce risk, improve resilience and build trust.



MythsLane

IT & Cyber Security Solutions Consulting

www.mythslane.uk



MythsLane

IT & Cyber Security Solutions Consulting

www.mythslane.uk

STRONG DNS. SECURE EMAIL. TRUSTED DOMAINS. RESILIENT BUSINESS.