The 10-Point DNS & Email Security Checklist

A Business Owner’s Guide to Preventing Domain Hijacking and Improving Deliverability

SPF

DKIM

DMARC

Presented by PORT::ZERO Cyber Solutions, LLC | 2026 Edition

The Stakes

Why Your DNS is the "Front Door" to Your Business

In the modern threat landscape, identity is the new perimeter. Attackers don't just hack into your servers; they spoof your identity to trick your employees, partners, and customers.

- 68% of breaches involve a human element (Social Engineering).
- Email remains the #1 vector for ransomware delivery.
- Misconfigured DNS is the leading cause of "Shadow IT" vulnerabilities.

This checklist is designed to help you audit your technical defenses so you can focus on growing your business.

Disclaimer: *This guide is for informational purposes. DNS changes can affect email delivery; always consult with a professional (like PORT::ZERO Cyber Solutions) before modifying production records.*

Phase 1 – Authentication & Identity

1. [ ] Audit Your SPF Record

- The Check: Do you have exactly one TXT record that starts with "v=spf1"?
- The Goal: Prevent unauthorized IP addresses from sending mail on your behalf.
- **Pro-Tip:** If you have multiple SPF records, they will both fail. Merge them into one.

2. [ ] Verify DKIM Signing

- The Check: Check your email headers for a DKIM-Signature.
- The Goal: Use "digital wax seals" to prove your messages haven't been tampered with in transit.

3. [ ] Harden Your DMARC Policy

- The Check: Is your policy set to p=quarantine or p=reject?
- The Goal: Moving beyond p=none is the only way to actually stop spoofed emails from reaching your clients' inboxes.

4. [ ] Enable DMARC Reporting (RUA)

- The Check: Do you have an rua=mailto: tag in your DMARC record?
- The Goal: You can't fix what you can't see. Monitoring reports tell you exactly who is trying to impersonate your domain.

Pro Tip: Don't try to read raw XML DMARC reports manually. We recommend using MXToolbox's DMARC Delivery Report tool. Simply enter your domain to see a clear visualization of who passes or fails your security checks.

Phase 2 – Infrastructure & Defense

5. [ ] Clean Up "Orphaned" DNS Records

- The Check: Delete CNAME or TXT records for services you no longer use.
- The Goal: Prevent "Subdomain Takeover" attacks.

6. [ ] Implement DNSSEC

- The Check: Enable DNS Security Extensions at your registrar (e.g., GoDaddy).
- The Goal: Protect your clients from "DNS Poisoning" that redirects them to malicious clone sites.

DNSSEC - Domain Name System Security Extensions

SPF - Sender Policy Framework

DKIM - DomainKeys Identified Mail

7. [ ] Enforce Registrar-Level MFA

- The Check: Is your Domain account protected by an Authenticator App?
- The Goal: If an attacker gains access to your registrar, they own your entire digital presence. SMS is not enough.

8. [ ] Check for MX Record Redundancy

- The Check: Ensure your Mail Exchange records point only to your active provider.
- The Goal: Minimize the attack surface for mail routing vulnerabilities.

DMARC - Domain-based Message Authentication, Reporting, and Conformance

RUA - Report URI for Aggregate Data

MX - Mail Exchange

Phase 3 – Maintenance

9. [ ] Check for DNS Propagation & Blacklisting

- The Check: Run your domain through a global blacklist engine to see if your mail servers have been flagged for spam or suspicious activity.
- The Goal: Ensure your IP reputation remains clean so that your critical business emails are actually delivered to your clients' inboxes rather than being silently blocked.

10. [ ] Perform a Quarterly DNS Audit

- The Check: When was the last time you cleaned up your TXT records?
- The Goal: Treat DNS like a garden; if you don't weed it, vulnerabilities will grow.

Next Steps

Technical Security is Only Half the Battle.

Even with a perfect DNS setup, the "Human Element" remains your largest vulnerability. A single employee clicking a sophisticated phishing link can bypass even the strongest technical controls.

Build Your Human Firewall with PORT::ZERO

While we engineer our **Incident Response Command Suite**, we are currently offering high-impact **Cybersecurity Awareness Training** tailored for small to mid-sized teams.

- Phishing Simulations (Real-world testing)
- Interactive Workshops (No boring PowerPoints)
- Executive Briefings (Risk management for leaders)

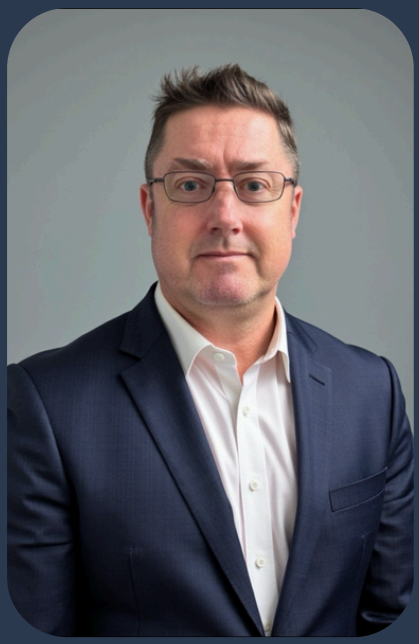
Technical Audit Tool: Use MXToolbox to verify these records. It’s the same tool we use at **PORT::ZERO** to ensure your "Human Firewall" isn't being bypassed by technical misconfigurations.

The Face Behind the Mission

Cybersecurity isn't just about code; it's about defense, discipline, and duty.

With a 35-year career spanning the U.S. Army, DoD Contracting, and Law Enforcement, I have dedicated my life to protecting what matters most. Most recently, I served as a Cybersecurity Advisor for 270+ agencies across South Carolina, leading incident response planning, numerous tabletop exercises, phishing campaigns, and creating training videos on offensive and defensive cyber tools and techniques.

I founded PORT::ZERO Cyber Solutions to bring that same high-stakes state and federal expertise to your organization.



Secure Your Team Today

Click here to schedule a 15-minute training discovery call

LinkedIn

YouTube

www.portzerocyber.com | rgkelly@portzerocyber.com | (877) 317-4422