■ DNS Health Check Checklist

Purpose: Make sure your domain isn't costing you money, losing emails, or leaving you vulnerable.

■ Step 1 – Domain Basics

■ Confirm your domain is registered in your name (not your web developer's).

■ Log in to your DNS manager (registrar, cPanel, or hosting provider).

■ Record when your domain expires (set a calendar reminder).

■ Step 2 – Email Records (MX)

■ Check which service is handling email (Microsoft 365, Google Workspace, or registrar-hosted).

■ Make sure only one set of MX records exists (duplicates = paying twice).

■ Confirm priority values are correct (lower numbers = higher priority).

■ Test email delivery by sending to/from external accounts.

■ Step 3 – Website Records (A & CNAME)

■ Your A record points to the correct web host IP.

■ Subdomains (blog, shop, portal) use CNAME records, not duplicate A records.

■ Old/unused records are deleted (no "mystery" IPs).

■ Step 4 – Security Records (TXT)

■ SPF record includes only your valid mail servers (e.g., Microsoft 365 or Google, not both).

■ DKIM is enabled for your email provider.

■ DMARC record exists with at least p=none (monitoring mode).

■ No multiple/conflicting SPF records.

■ Step 5 – Test Your Setup

■ Run your domain through MXToolbox.com.

■ Fix any critical errors (red flags).

■ Verify SPF, DKIM, and DMARC pass when sending test emails.

■ Step 6 – Maintenance

■ Review DNS records at least once a year.

■ Remove old entries when changing providers.

■ Document your DNS setup in a shared IT file.

■ Final Tip

■ Misconfigured DNS isn’t just annoying — it can cost you money (double email hosting), lost clients (emails bouncing),