Everyday Soul — CyberScrolls Series

EP04 – Track the Tricksters with MXToolbox

By Helen Najar | Lionheart

Guides and reflections for unmasking email tricksters—seeing past the sender name to the truth beneath.

⚡ Quick Checks — If You Only Have 60 Seconds

1. **Copy the sender's domain** (everything after the @).
2. **Open** https://mxtoolbox.com
3. **Run** "MX Lookup" on the domain.
4. **Check SPF & DMARC:** run "SPF Record Lookup" and "DMARC Lookup."
5. **Open "Email Health"** for a quick scan: errors, missing records, misconfigurations.
   If SPF/DMARC are missing or records look broken, do not trust the email.

Keep this page bookmarked. Do the quick actions now, then read the full steps below.

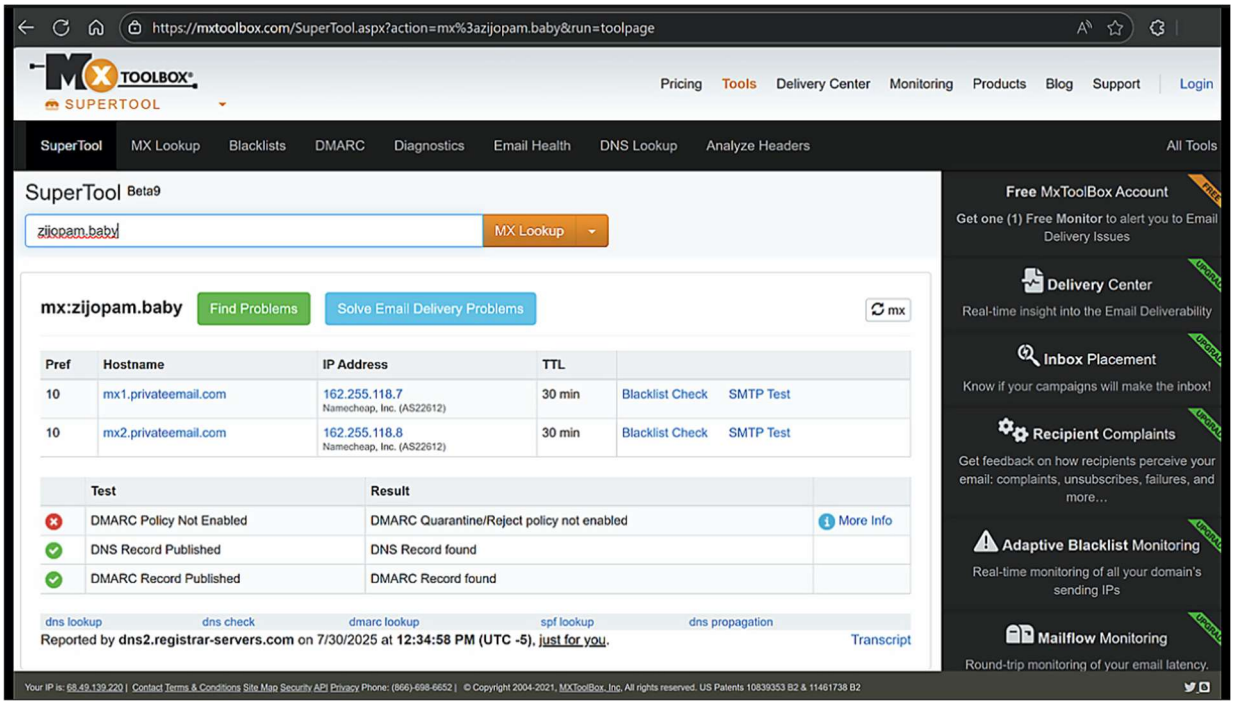
Full Guide — Unmasking the Sender

1. Extract the Domain

- From the suspicious sender, copy the domain (e.g., alerts@copam.baby → copam.baby).
- Ignore display names; focus on the domain itself.

2. MX Lookup (Mail Exchange)

- What you're checking: Who handles email for this domain?
- Red flags: No MX records; bizarre or throwaway providers; mismatched infrastructure.



Truth hides in headers — not names.

3. SPF Record Lookup

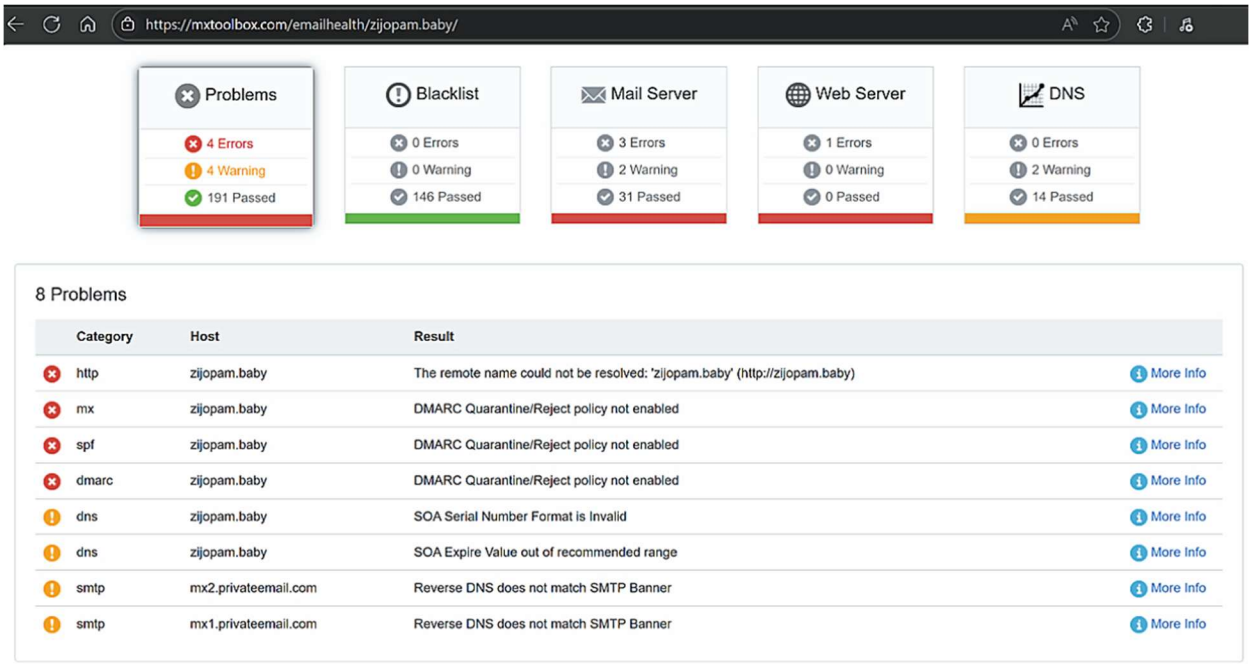
- What it is: **The guest list** for senders.
- Good sign: An SPF record exists and lists legitimate senders.
- Red flags: No SPF; overly permissive records (e.g., +all).

4. MARC Lookup (and note DKIM alignment)

- What it is: The enforcer—policy for failed checks.
- Good sign: A valid DMARC record with an enforcement policy (quarantine/reject) and proper alignment.
- ed flags: No DMARC; p=none on obviously risky domains; misaligned or missing DKIM/SPF.

5. Email Health Scan

- Click Email Health in MXToolbox for the domain.
- Let the tool run; review errors/warnings: missing SPF/DMARC, DNS issues, misconfigurations.
- Use this to confirm your suspicion before you act.



Every missing record leaves a crack in the armor

6. Reflection — the Lionheart reminder

"It's not the name that proves the truth— it's the bones beneath it.
Read the records. Guard your helm."

Appendix — Quick Links

- **MXToolbox:** https://mxtoolbox.com
- **SPF Record Lookup:** MXToolbox → "SuperTool" → spf:domain.com
- **DMARC Lookup:** MXToolbox → "SuperTool" → dmarc:domain.com
- **Email Health:** MXToolbox → "Email Health" → enter domain