

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.

EP04 – Track the Tricksters with MXToolbox	0
Full Guide — Unmasking the Sender	1
1. Extract the Domain	1
2. MX Lookup (Mail Exchange).....	1
3. SPF Record Lookup	1
4. MARC Lookup (and note DKIM alignment).....	2
5. Email Health Scan	2
6. Reflection — the Lionheart reminder	3
Appendix — Quick Links.....	3

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.

The screenshot shows the MXToolbox SuperTool interface. In the search bar, 'zijopam.baby' is entered. Below the search bar, there are two buttons: 'Find Problems' and 'Solve Email Delivery Problems'. The main results section is titled 'mx:zijopam.baby' and contains a table with two rows of MX records:

Pref	Hostname	IP Address	TTL	Blacklist Check	SMTP Test
10	mx1.privateemail.com	162.255.118.7 Namecheap, Inc. (AS22612)	30 min	Blacklist Check	SMTP Test
10	mx2.privateemail.com	162.255.118.8 Namecheap, Inc. (AS22612)	30 min	Blacklist Check	SMTP Test

Below the table, there's a 'Test' section with three items:

- DMARC Policy Not Enabled (with a red X icon)
- DNS Record Published (with a green checkmark icon)
- DMARC Record Published (with a green checkmark icon)

At the bottom of the results page, there are links for 'dns lookup', 'dns check', 'dmarc lookup', 'spf lookup', and 'dns propagation'. A note says 'Reported by dns2.registrar-servers.com on 7/30/2025 at 12:34:58 PM (UTC -5). just for you.' To the right of the results, there are promotional banners for 'Free MxToolBox Account', 'Delivery Center', 'Inbox Placement', 'Recipient Complaints', 'Adaptive Blacklist Monitoring', and 'Mailflow Monitoring'.

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.
- Red 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.

The screenshot shows the MXToolbox Email Health Scan interface. At the top, there are five summary boxes: 'Problems' (4 Errors, 4 Warnings, 191 Passed), 'Blacklist' (0 Errors, 0 Warnings, 146 Passed), 'Mail Server' (3 Errors, 2 Warnings, 31 Passed), 'Web Server' (1 Error, 0 Warnings, 0 Passed), and 'DNS' (0 Errors, 2 Warnings, 14 Passed). Below this, a section titled '8 Problems' lists the following findings:

Category	Host	Result	Action
✖ http	zjopam.baby	The remote name could not be resolved: 'zjopam.baby' (http://zjopam.baby)	More Info
✖ mx	zjopam.baby	DMARC Quarantine/Reject policy not enabled	More Info
✖ spf	zjopam.baby	DMARC Quarantine/Reject policy not enabled	More Info
✖ dmarc	zjopam.baby	DMARC Quarantine/Reject policy not enabled	More Info
⚠ dns	zjopam.baby	SOA Serial Number Format is Invalid	More Info
⚠ dns	zjopam.baby	SOA Expire Value out of recommended range	More Info
⚠ smtp	mx2.privateemail.com	Reverse DNS does not match SMTP Banner	More Info
⚠ smtp	mx1.privateemail.com	Reverse DNS does not match SMTP Banner	More Info

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](https://mxtoolbox.com/SuperTool/SPFR.aspx)
- **DMARC Lookup:** MXToolbox → “SuperTool” → [dmarc:domain.com](https://mxtoolbox.com/SuperTool/DMARCLookup.aspx)
- **Email Health:** MXToolbox → “Email Health” → enter domain