Postbox Services
YOUR EMAILING PARTNER

POSTBOX SERVICES · DESK REFERENCE

Spot a spoofed email in 30 seconds

The sender name is easy to fake. The headers are the receipts - five places a spoof always gives itself away.

1 Authentication-Results fails

The receiving server's own verdict on SPF, DKIM and DMARC. Genuine mail passes all three, aligned to the From domain. A failure here is the loudest alarm.

```
want: spf=pass · dkim=pass · dmarc=pass  |  alarm: fail / none
```

2 From vs Return-Path mismatch

The From is what you see; the Return-Path is where bounces really go. Genuine mail keeps both in the same organisation - a spoof shows your bank up front, a throwaway domain underneath.

```
From: yourbank.com  Return-Path: mailer-3x9.top
```

3 Display-name & lookalike tricks

A trusted name pasted in front of an unrelated address, or a domain one character off so it reads right at a glance. Check the actual address, character by character.

```
"PayPal Support" <alerts@random-mail.xyz>  ·  paypa1.com
```

4 Suspicious Received chain

Read the Received lines bottom-up - the lowest is the true origin. Mail "from your CEO" that started on an unknown foreign server is not from your CEO.

```
Received: from mailer-3x9.top (45.148.10.77)
```

5 Reply-To redirection

A Reply-To that differs from the From quietly hijacks your reply to an attacker's inbox. The classic CEO-fraud move, paired with urgency and a payment request.

```
From: ceo@yourcompany.com  Reply-To: ceo.urgent@gmail.com
```

The 30-second red-flag checklist

- [ ] spf=fail, dkim=none or dmarc=fail for the From domain
- [ ] Return-Path domain does not match the From domain
- [ ] Display name and actual address belong to different organisations
- [ ] From domain is a near-miss of a real one (swapped or added characters)
- [ ] Oldest Received hop has no connection to the claimed sender
- [ ] Reply-To points somewhere other than the From address
- [ ] Any of the above + urgency, secrecy, or a money / credentials request

Any box ticked? Treat it as suspect - verify through a known channel (never by replying) and report it to your IT / security team.

Paste the headers, get the verdict in seconds - free, no signup
mx.postboxservices.com/email-header-analyzer
Grades SPF, DKIM and DMARC + maps the delivery path hop by hop

Postbox Services
Full guide: postboxservices.com/blogs