# Email Verification Checklist

Use for invoices, account alerts, “shared document” messages and anything that asks for action.

**Keep it safe**

**Do not paste suspicious links or attachments into this form.** Describe them in your own words. Never type passwords or full account numbers here.

| | |
|---|---|
| **Date and time received** | |
| **Who it claims to be from** | |
| **Sender’s actual email address (as shown when you open details)** | |
| **What it asks me to do** | |

## Quick checks (tick each one you have done)

- ☐ The **actual sender address** matches the real organization (watch for look-alikes: rnicrosoft, paypa1, extra words, odd endings).
- ☐ I was **expecting** this invoice, document or alert.
- ☐ The greeting and writing look normal for this sender (no odd wording, generic “Dear customer”).
- ☐ I have **not clicked** anything. On a computer I hovered over the link and the address matches the company; on a phone I did not tap it.
- ☐ The attachment is a type I expected (be cautious with zip, html, macro-enabled Office files, or unexpected PDFs).
- ☐ The message does **not** pressure me with a deadline, a threat or a “secret”.
- ☐ Payment details (bank, e-transfer address) are **unchanged** from past invoices — or I have confirmed the change by phone.

## Second-channel check

- ☐ I contacted the sender by phone or app using details I already had.
- ☐ They confirmed they sent it.

## Result

- ☐ Verified as genuine
- ☐ Suspicious — deleted and reported (mark as phishing in your email app; forward to your provider or employer’s security team)
- ☐ Not sure — asked a second family member

## Notes


© 2026 Cogitent Press. All rights reserved. Educational use only; not legal or financial advice.