

Visual breakdown – suspicious elements in an AI phishing email

Left: example email (mock). Right: annotated suspicious elements with quick checks you can run.

AT Amazon Payroll
payroll@amazn-support-secure.com

Action required: Update your payment method to avoid suspension

We noticed unusual activity in your account. To avoid intrusion, confirm your billing details using the secure link below.

Hi Karan,
We could not validate your recent payment. Please update your payment information immediately to avoid service disruption. **Failure to update within 24 hours will result in account suspension.**
Click here to update: [amazn-support.online/update](#)

Update payment

If you did not request this, ignore this email.
For help contact [support@amazn.com](#)

- 1. Trusted name ≠ trusted email**
A familiar display name can mask a suspicious domain (e.g., [amazn-support-secure.com](#)). Always check for misspellings, extra hyphens, or added words—hover to reveal the real sender.
- 2. Visual flaws = warning signs**
Poor grammar, odd fonts, or blurry logos often signal a spoofed message. Stay alert to these subtle cues.
- 3. Generic greeting = AI clue**
Oddly formal tone or greetings like “Hi Karan” may signal automated content. Watch for unnatural phrasing or excessive politeness.
- 4. Urgency ≠ legitimacy**
Threats like “**update within 24 hours**” are pressure tactics. Real providers rarely rush or threaten—always verify through your official account.
- 5. Links can lie**
Hover before clicking. A link like [amazn-support.online/update](#) may look safe but lead elsewhere. Never enter credentials unless the site is verified.
- 6. Attachments & buttons = caution**
Unexpected files or “Update” buttons can be risky. Scan before opening, and log in directly—don’t click through the email.
- 7. Mixed contact info = red flag**
If the footer says [support@amazn.com](#) but the sender domain doesn’t match, it’s likely a scam.