

Spot and report a suspicious message

A calm, repeatable check for unexpected emails, payment changes, QR codes and sign-in requests.

4 min read | Reviewed 15 October 2026

BEFORE YOU START

Know your company's reporting route and a trusted telephone number for your IT team. Payment approvers should have an independently maintained supplier contact list.

01 Pause before interacting

Treat unexpected urgency, a changed bank account, a password request or an unfamiliar attachment as a reason to pause. A familiar display name or polished logo is not enough to trust a message.

Do not open the attachment, scan its QR code, reply or enter credentials to investigate. On a phone, avoid tapping a link just to see where it leads.

02 Verify through another route

For a payment or sensitive-data request, call the person using a number already in your records. Do not use the number or contact button supplied in the suspicious message.

If the request appears to come from a colleague, confirm it in person or through a known channel. Continue the normal approval process even if the sender claims an exception is urgent.

03 Report, then follow guidance

In supported, configured Outlook versions, select the message, then Report and Report phishing. If that option is absent, use your organisation's reporting process; do not forward a live attachment widely.

If you clicked, shared information or approved a sign-in, contact IT promptly and say exactly what happened. Reporting a message alone does not resolve a potentially compromised account.

Your practical checklist

Spot and report a suspicious message

- ☐ No further interaction with the suspicious content
- ☐ Sender/request independently checked where necessary
- ☐ Payment approval controls retained
- ☐ Message reported using the agreed route
- ☐ Any click or information disclosure reported to IT
- ☐ Follow-up instructions and reference recorded

Record the next action

Message date, subject and reporting time (no sensitive content)

Support reference and assigned owner

Next action / agreed follow-up time

A message can be malicious without spelling mistakes. If money may have been transferred, alert the authorised finance lead immediately using a trusted channel.

OFFICIAL SOURCES & FURTHER READING

Microsoft: protect yourself from phishing

Microsoft: report suspicious messages in Outlook

Links open the official source. Web edition: compurep.co.za/guides/spot-and-report-phishing