Recognize a phishing email

The 5 signs that give a fraudulent message away — and the 60-second rule.

THE 5 SIGNS

1 — The real address doesn't match
Look at the sender's full address, not the displayed name: paypall.com is not paypal.com.

2 — Artificial urgency
“Within 24h”, “immediate action”: the pressure itself is the alarm signal.

3 — The link doesn't lead where it shows
Hover without clicking: the real destination appears at the bottom. Long-press on mobile.

4 — Unexpected attachment
The main ransomware vector. Confirm through another channel before opening — and back up your files.

5 — Request for sensitive information
No legitimate organization asks for passwords or card numbers by email.

The 60-second rule

1. Close the email — no reply, no click.
2. Open a new tab and go to the official site yourself.
3. Check whether the problem really exists. Almost always: it doesn't.

Urgency is their weapon. Time is yours.

Report and react

UK: report@phishing.gov.uk · texts 7726 — US: ic3.gov (FBI) · reportfraud.ftc.gov (FTC)
Attachment opened by mistake: antivirus scan + change your passwords.
EU help: FR cybermalveillance.gouv.fr · ES 017 (INCIBE) · BG cybercrime.bg