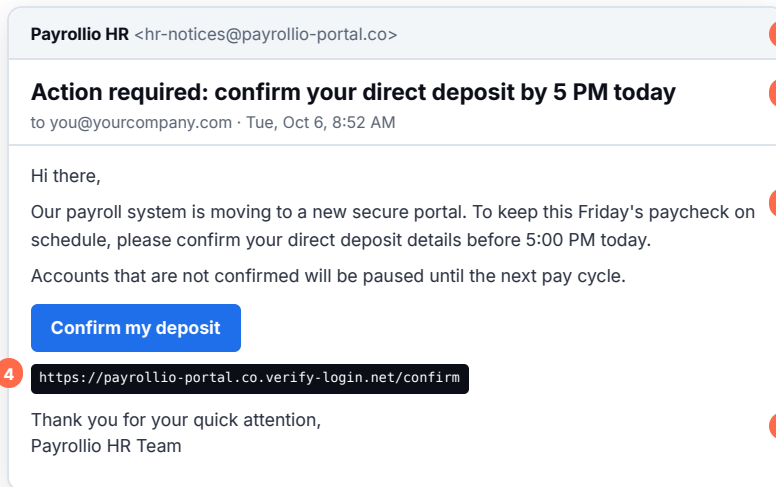


EMAIL · TEXT · CHAT · PHONE

How to spot a phishing message

Bad spelling used to give phishing away. AI fixed that for attackers. Today the tell is what the message wants from you, and how hard it pushes.



- 1 Lookalike sender**
It says HR, but the address is an outside "portal" domain you've never used.
- 2 Pressure + deadline**
"By 5 PM today" and a paused paycheck. Classic.
- 3 Moves money or access**
It wants your login and bank details.
- 4 Link goes somewhere else**
Hover the button: the real address is a different site.
- 5 Flawless grammar**
Polished writing is not a pass.

1 Pressure

"Act now." "Within 24 hours." "Before your account closes." Urgency is built to make you skip the part where you think.

2 A request that moves money or access

Gift cards, a wire, new bank details for payroll or a vendor, your passphrase, or an MFA code. Those are the prizes.

3 Secrecy or a detour

"Keep this between us." "I'm in a meeting, just text me." Attackers love pulling you away from the normal process.

4 Sender or link doesn't match

Check the real address, not just the display name. Hover (or long-press on a phone) to see where a link actually goes. Lookalike domains swap a letter or add a word.

5 A surprise

A delivery you didn't order, a reset you didn't request, an invoice from a vendor you don't use, a QR code in an email.

6 Perfect grammar proves nothing

Clean, friendly writing is free now. Don't let polish earn trust.

What to do

Don't click, reply, or scan. Report it with your report button or send it to IT. Then check through a channel you already trust: a known phone number, the real app, or walking over to ask.