SPOT THE PHISHING EMAIL (Quick Checklist)

Before clicking any email link, take 10 seconds to check

1 CHECK THE SENDER

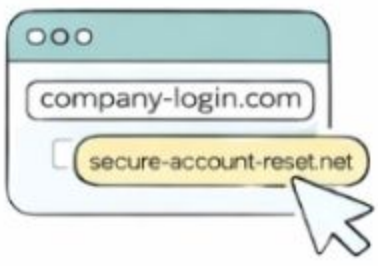
- Is the email address correct?
- Look for extra words or strange domains
- Example:
  hr@company.com ✓
  hr@company-security.com ✗

2 LOOK FOR URGENCY

Phishing emails often pressure you to act quickly.
Examples:

- "Act immediately"
- "Your account will be locked"
- "Urgent request from management"

If it feels rushed, pause first.



3 HOVER BEFORE YOU CLICK

Place your mouse over the link to see the real destination.
Displayed link:
company-login.com
Actual link:
secure-account-reset.net
If the destination looks suspicious → Do not click.

4 CHECK THE MESSAGE QUALITY

Warning signs include:

- Generic greetings ("Dear User")
- Spelling or grammar mistakes
- Unexpected attachments

5 WHEN IN DOUBT – REPORT IT

Forward suspicious emails to your IT Security Team.

Reporting helps protect everyone.