

Recognizing Red Flags

What Are “Red Flags”?

- Red flags are ***warning signs*** that a message might be fake.
- Attackers add small hints that don't look normal.
- Learning these signs helps stop the attack early.
- Always pause before clicking anything.

Red Flag #1: Suspicious Sender

- Email address looks almost correct but slightly different.
- Unknown sender claiming to be someone important.
- Free email domains used for official messages.
- No profile picture or unclear name.

Red Flag #2: Unexpected Urgency

- Attackers push you to act *fast*.
- Words like “urgent”, “immediately”, “account locked”.
- Pressure causes mistakes.
- Real organizations rarely rush you like this.

Red Flag #3: Strange Links & Attachments

- Links don't match the real website.
- Attachments you weren't expecting.
- Files pretending to be salary slips, invoices, reports.
- Hovering over links shows the real suspicious URL.

Red Flag #4: Poor Language & Formatting

- Spelling or grammar mistakes.
- Logo looks stretched or low quality.
- Odd greetings like “Dear User” or “Hello Customer”.
- Professional companies rarely send messy emails.

Complete Red Flag Scenario — Spot the Phishing Signs

Suspicious
sender



it-support@company-secure-login.com
To: Hassan

Your account will be blocked in 10 minutes!

Dear Hassan,
Your account will be blocked in 10 minutes!

Verify Now

Strange link

Enter your password to continue.

Request for sensitive info