

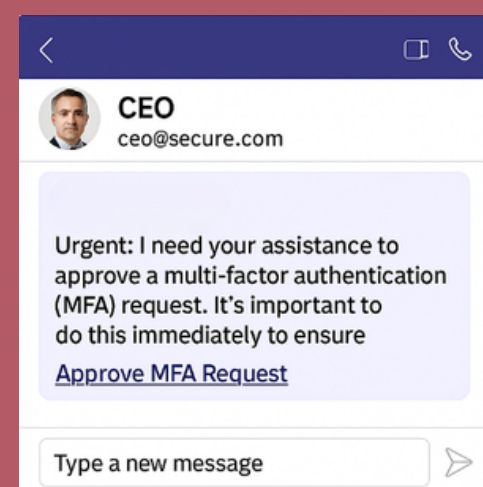
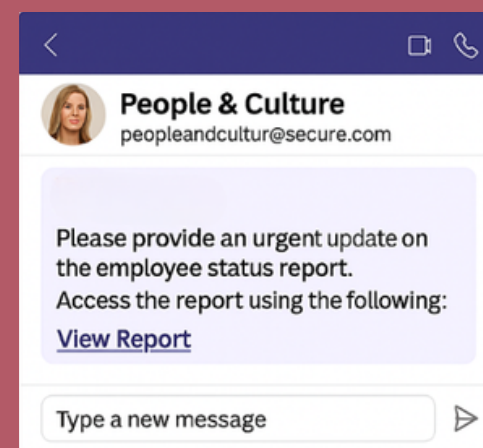
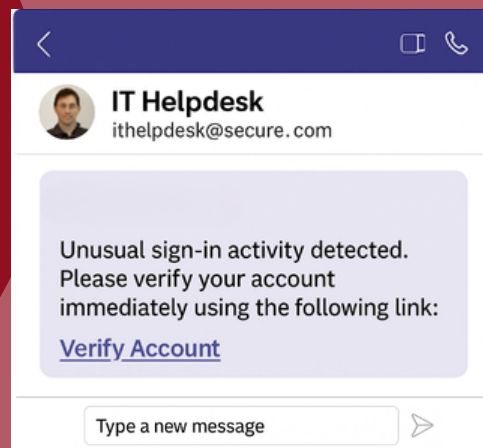


# Stop Chat Phishing Scams

Spot suspicious messages.  
Verify the sender. Report the attempt.



Could these messages be fake?



## Spot the warning signs

### IMPERSONATION

Claims to be IT, HR, a senior leader or a colleague.

### UNEXPECTED MESSAGE

Comes from someone you do not recognise or were not expecting.

### URGENCY OR PRESSURE

Pushes you to act quickly, approve something or keep it quiet.

### SUSPICIOUS LINKS OR FILES

Asks you to verify an account, reset a password or open a document.

### REQUESTS TO MOVE CHANNELS

Asks you to switch to personal email, SMS or another app.

## Pause, check & report

### SCAN FOR S.C.A.M.

Check the **Sender**, **Content**, **Action** and **Manage** the message safely.

### DO NOT ACT STRAIGHT AWAY

Pause before replying, clicking, approving or sharing information.

### VERIFY THROUGH A TRUSTED CHANNEL

Use known contact details or an approved internal process to check unusual requests.

### NEVER SHARE PASSWORDS OR MFA CODES

These should not be shared through chat.

### REPORT SUSPICIOUS ACTIVITY

Use your organisation's usual reporting process.

Chat phishing uses workplace messaging tools to impersonate trusted people and pressure employees into acting before checking.

See something suspicious? Pause and report it.