1. GENERIC EMAIL PHISHING

Generic phishing involves sending the same scam email to thousands of people at once, hoping someone falls for it.

These emails are not personalized and rely on sheer volume to trick victims.

What Is Generic Email Phishing?

Generic phishing is mass-emailed scams sent to thousands of users hoping someone clicks.

Scenario: Hassan Receives a Fake IT Alert

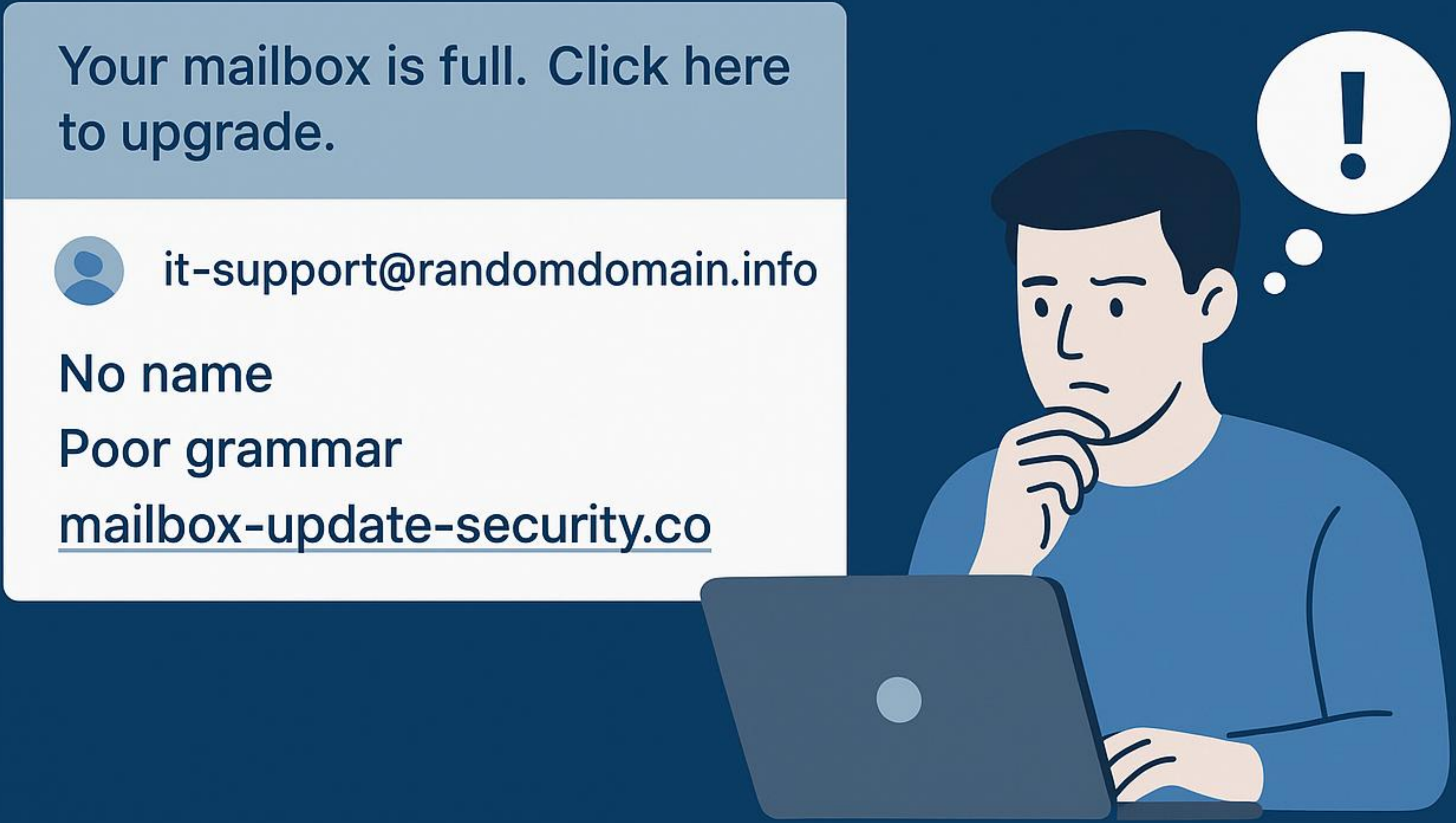
Hassan gets an email:
“Your mailbox is full. Click here to upgrade.”

- No name
- Poor grammar
- Suspicious link mailbox-update-security.co

He almost clicks but notices the sender is **"it-support@randomdomain.info"**.

Lesson: Mass emails rely on urgency + confusion.

Scenario: Hassan Receives a Fake IT Alert



Your mailbox is full. Click here to upgrade.

it-support@randomdomain.info

No name

Poor grammar

mailbox-update-security.co

How Attackers Trick Employees?

Common tactics:

- Urgent warnings
- Prize or reward emails
- Fake password expiry alerts
- Fake delivery notifications

How to Avoid Generic Phishing?

- Inspect sender domain
- Hover over links
- Never download unsolicited attachments
- When unsure → contact IT

Why Generic Phishing Still Works?

Because attackers need just **one employee** to make a mistake, these mass phishing emails can still be very effective.