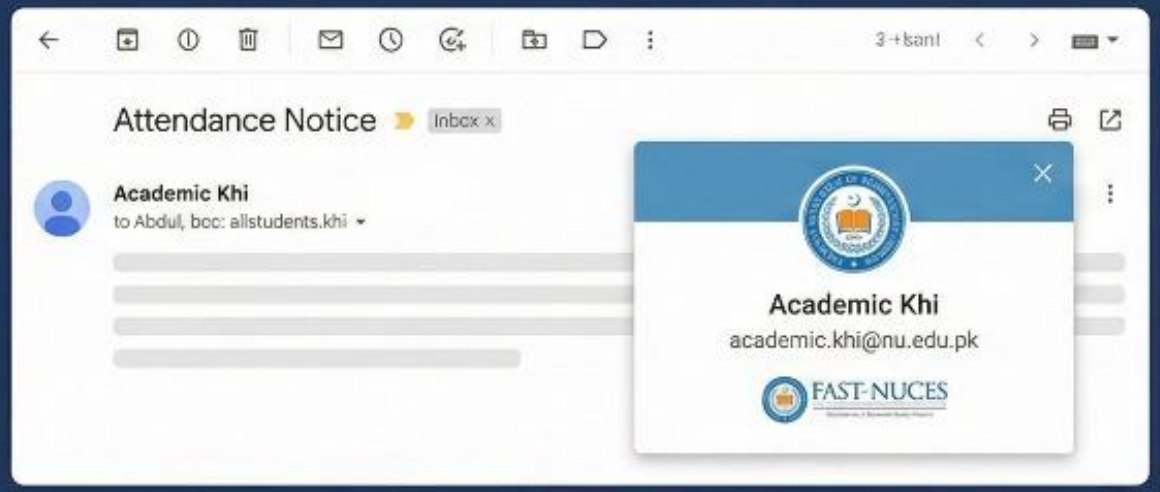
ROLE-SPECIFIC SCENARIOS

Why Role-Based Awareness Matters

- Different people in an organization face different phishing risks.
- Understanding your **role** helps you avoid the attacks designed for you.
- “One size fits all” doesn’t work for cybersecurity.

Maryam Receives a Phishing Email



Scenario for Students (Maryam)

Maryam, a student, receives an email saying:
"Your course registration will be cancelled. Click here to confirm your CNIC and fee slip."

Red Flags:

- Fear-based message
- Asking for personal documents
- Suspicious link

Correct Action:

Maryam reports it and logs in through the official FAST portal instead of clicking.

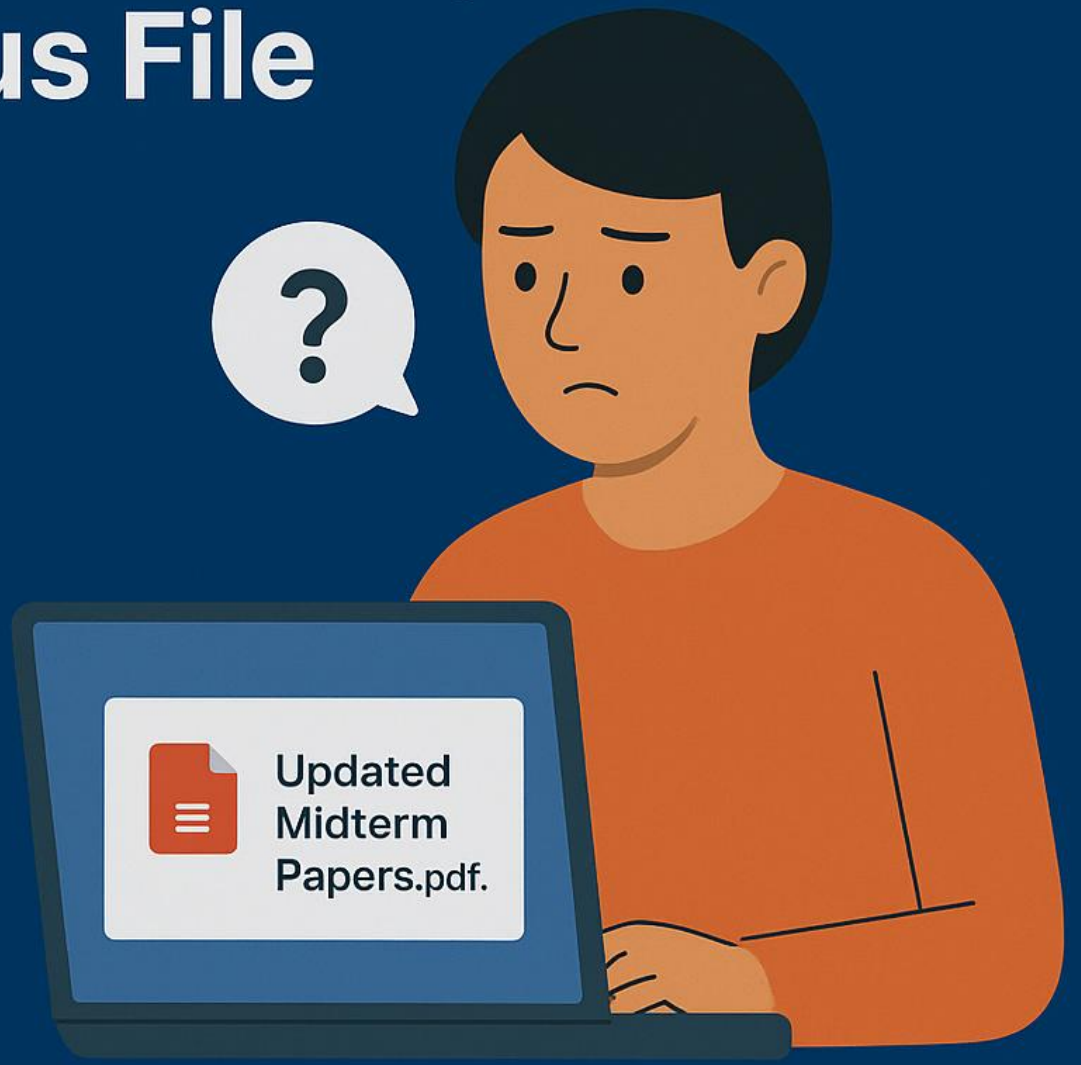
Hassan, a TA/Instructor, Gets a Suspicious File

Red Flags:

- Wrong file type
- Unusual sender
- Unexpected update

› Hassan verifies with the course coordinator before opening

→ **Attack blocked.**



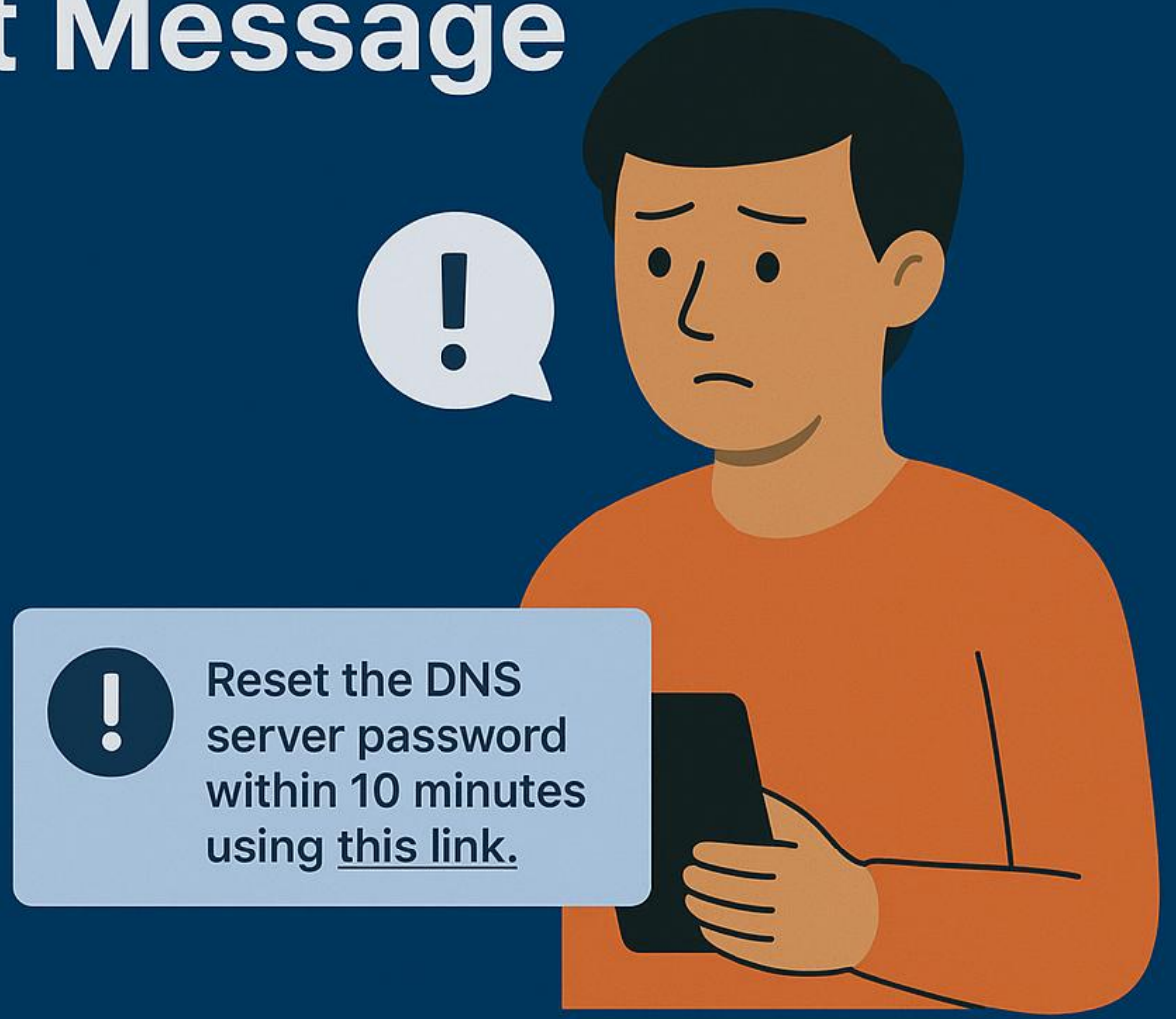
Arham, an IT Helper/Admin, Gets an Urgent Message

Red Flags:

- Extreme urgency
- Untrusted link
- High-impact request

› Arham checks with his supervisor and uses official tools

→ **Attack blocked.**



Finance / HR Scenario

An HR officer gets a message:

“Download all employee CNICs and salary slips urgently for audit.”

Red Flags:

- Sensitive data request
- Unknown sender
- “Urgent” pressure

Correct Action:
HR verifies with department head → It was a phishing email.

Key Message

- Attackers study your **job role** to design better scams.
- Always verify unexpected requests related to:

✓ Password resets
✓ Salary or money
✓ Student data
✓ System access

- When unsure → **ASK. Don’t click!**