🔴 Risk Classification: Phishing

Reason:

This email shows multiple confirmed phishing indicators, including a fake sender domain, malicious-looking link, urgency-based language, generic greeting, and failed email authentication checks. If interacted with, it could lead to credential theft or unauthorized account access.

How the Attack Works

This email is designed to trick the recipient into thinking their account is in danger. By clicking the link and entering personal information, the user may unknowingly give their login details to attackers. The email uses urgency, fear, and a fake sender domain to make the message seem legitimate, which are common tactics in phishing attacks.

Prevention & Awareness Guidelines

How to Avoid Phishing Emails

- Always check the sender’s email address carefully before taking action.
- Be cautious of emails that create urgency or threaten negative consequences.
- Do not click links or download attachments from unknown or untrusted sources.
- Hover over links to inspect the URL before clicking.
- Verify suspicious messages through official channels before responding.

What to Do If You Receive a Suspicious Email

- Do not reply to the email.

- Do not click any links or provide personal information.
- Report the email to the IT or security team.
- Delete the email after reporting it.

Do’s and Don’ts for Employees

Do’s

- Verify unexpected emails through official company channels.
- Check email sender addresses and links carefully.
- Report suspicious emails to the security or IT team immediately.
- Keep your passwords and login details private.

Don’ts

- Do not click on suspicious links or attachments.
- Do not share passwords, OTPs, or personal information via email.
- Do not respond to emails that pressure or threaten you.
- Do not assume an email is safe just because it looks professional.