



# Your Inbox Is NOT as Innocent as It Looks...

Phishing Awareness for HR & Marketing Teams

High Visibility

High Access

High Risk





# What is Phishing?



- Phishing is when attackers impersonate a trusted person or organization to trick you into giving up sensitive information.
- Attackers send fake links or attachments to install malware or tick you into sharing financial details, login credentials, or sensitive data.
- A successful phishing attack can cost companies millions and put employees at risk.



# Can You Spot Phishing Emails?



Keep an eye out for these **red** flags:

## Urgency

- “Act now.”
- “Your account will be locked.”

## Credential Request

- Ask's for:
  - Passwords
  - Identification

## Impersonation

- Pretends to be:
  - Manager
  - Payroll
  - IT support

## Suspicious Links

- Misspelled domains
- Extra numbers or characters
- Link does not match the preview

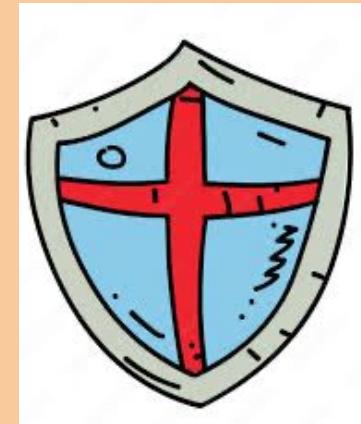


**THINK  
BEFORE YOU  
CLICK**



# How Do We Stop Getting Phished?

**Pause Before You Click** = STOP and THINK



**Check the Sender** = Look for typos

**Hover Over Links** = Confirm the URL

**NEVER Share Credentials** = Passwords, MFA Codes, ID

**Verify Requests** = Call First



**Report ANY Suspicious Emails** = Help protect everyone

