

PHISHING AWARENESS

# Protecting Our Organization



HARSHIT SOMANI





# Phishing Attack Awareness

In today's digital landscape, it is crucial to **understand the teams** most targeted by phishing attacks. Recent simulations have revealed that the HR and Marketing teams are often prime targets. Attackers frequently focus on roles that handle sensitive data, engage in external communications, or work with resumes and campaigns. Awareness is our strongest defense, and it is essential to empower these teams to recognize and respond to potential threats effectively.

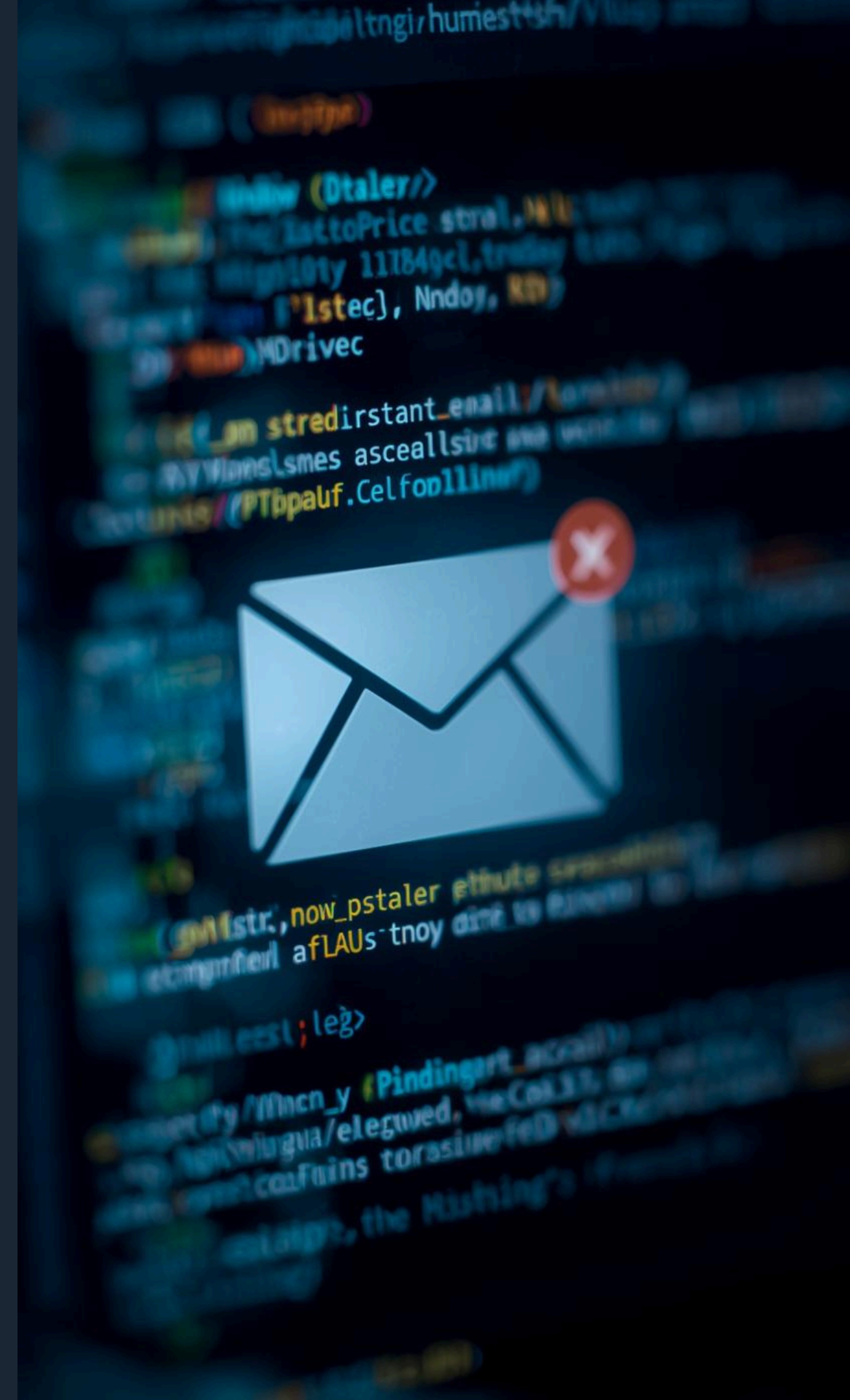
Phishing does not discriminate based on job titles; rather, it targets **human behaviors** that can be exploited. As the first line of defense, all employees must remain vigilant and educated about phishing tactics. Organizations should prioritize training for at-risk teams, equipping them with the necessary tools to handle suspicious communications. By fostering a culture of security awareness, we can mitigate risks and protect our valuable data from falling into the hands of cybercriminals.



# What Is Phishing?

Phishing refers to a **cyberattack strategy** where attackers impersonate trusted sources, such as IT, HR, and vendors, to manipulate individuals into revealing sensitive information. Phishing emails often appear genuine and create a sense of urgency. Their primary goal is to entice victims into clicking on malicious links or disclosing personal data, which can lead to severe consequences for both the individual and the organization. Awareness of this deceptive tactic is crucial in preventing successful attacks.

Understanding the deceptive nature of phishing is essential for protecting our organization. Attackers employ various techniques, making their emails look legitimate and professional. They often aim to exploit fear or urgency, pressuring recipients to act quickly without thinking. It's important to remember that **phishing emails are designed** to catch you off guard, prompting immediate action. By recognizing these tactics, we can empower ourselves to be vigilant and safeguard our sensitive information from potential threats.





# Common Phishing Tactics

## Key signs and typical tricks used

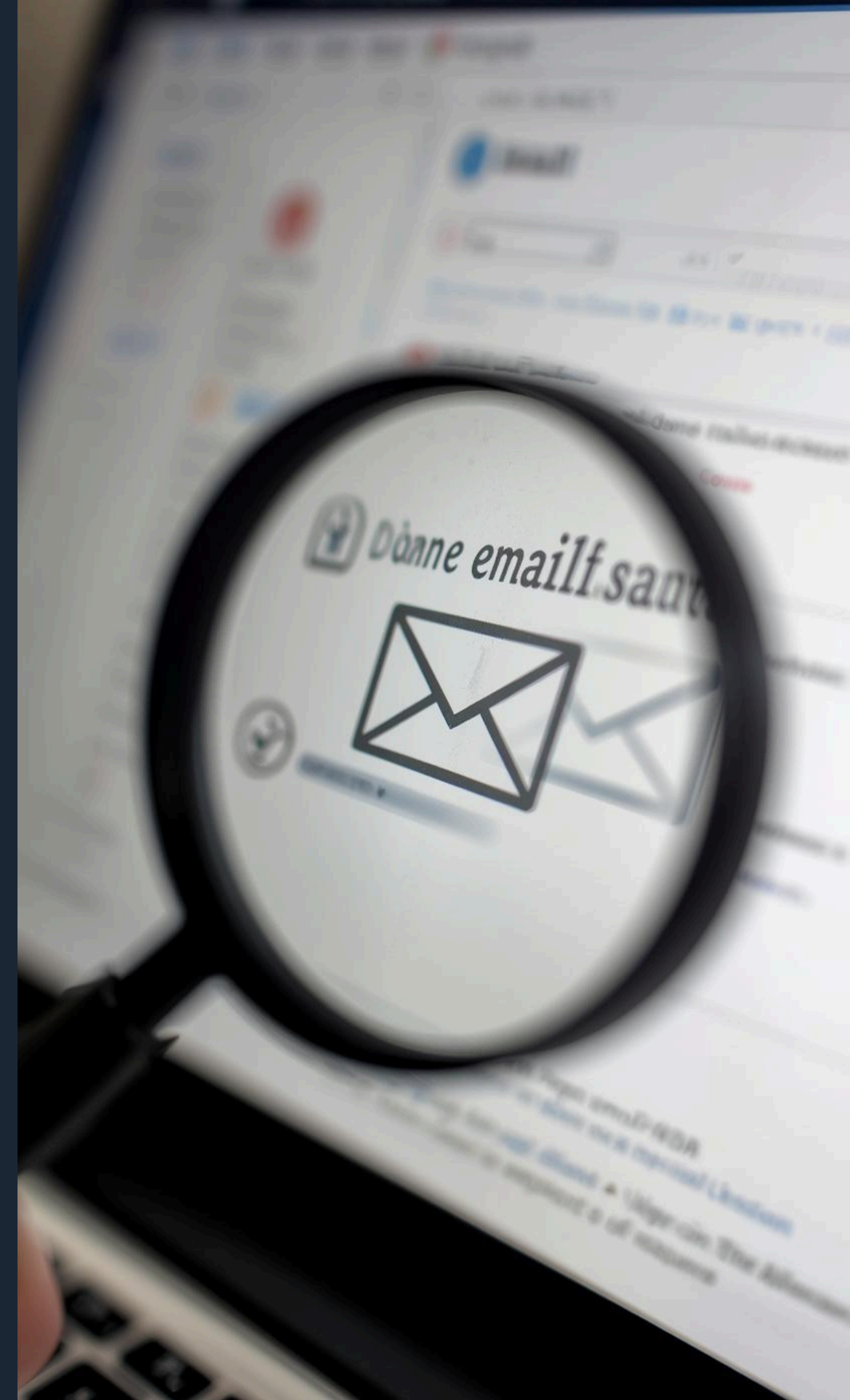
- Urgent language prompts immediate action
- Fake internal emails create confusion
- Generic greetings lack personalization
- Links that appear legitimate, but aren't
- Unexpected attachments can be harmful



# Spot Phishing Emails

## Key questions for email evaluation

- Is the sender's address correct?
- Is urgency created in the message?
- Were you expecting this email?
- Does the link match our domain?
- If unsure, treat as suspicious.



# Stop Getting Phished

## Practical steps for email safety

- Slow down – attackers rely on urgency
- Verify requests through another channel
- Never enter passwords via email links
- Report suspicious emails immediately
- It's okay to question emails



# Thank You for Your Attention

## Email

harshitsomani2005@gmail.com

## Social Media

<https://portfolio-neon-sigma-cvid3js03j.vercel.app/>

## Phone

9414832105

