Phishing Awareness Guide

1. What is Phishing?

Phishing is a type of cyberattack where attackers trick individuals into revealing sensitive information, such as passwords, credit card numbers, or personal details, by pretending to be trustworthy entities.

2. Common Signs of Phishing:

- Urgent or threatening language ('Your account will be closed!')
- Suspicious links or attachments
- Requests for personal or financial information
- Generic greetings like 'Dear Customer'
- Poor spelling and grammar mistakes

3. How to Stay Safe:

- Verify the sender's email address carefully.
- Hover over links before clicking to see the real destination.
- Never share sensitive information over email or phone calls.
- Enable Two-Factor Authentication (2FA) wherever possible.
- Report suspicious emails to your IT department.

4. Example of a Phishing Email:

> 'Dear Customer,

Your account has been suspended!

Click here immediately to verify your identity.'

(Notice the urgent tone and suspicious link.)

5. Conclusion:

Always think before you click.

Stay alert, verify sources, and protect your information!

Stay Safe Online!