# TASK 02:

# Phishing Awareness & Social Engineering Training

**Prepared for:** CodeAlpha Cybersecurity Internship

## INTRODUCTION TO PHISHING

- **Definition**: Phishing is a type of cyber attack where attackers pose as trusted entities to steal sensitive data like passwords and credit card numbers.
- **Goal**: To trick individuals into clicking malicious links or downloading dangerous attachments.
- **Impact**: Can lead to data breaches, financial loss, and unauthorized access to organizational systems.

## COMMON SOCIAL ENGINEERING TACTICS

- **Urgency**: Attackers use "Limited Time" or "Account Suspended" warnings to make you act without thinking.
- **Authority**: Posing as a CEO, IT manager, or government official to gain trust.
- **Curiosity**: Using topics like "Salary Increases" or "Leaked Photos" to bait clicks.
- **Fear**: Threatening legal action or account deletion if instructions aren't followed.

## HOW TO RECOGNIZE PHISHING EMAILS (RED FLAGS)

- **Sender Address**: Check for subtle misspellings (e.g., micros0ft.com instead of microsoft.com).
- **Generic Greetings**: Using "Dear Customer" instead of your actual name.
- **Suspicious Links**: Hover your mouse over a link to see the actual destination URL before clicking.
- **Poor Grammar**: Many phishing emails contain spelling mistakes and strange phrasing.

## REAL-WORLD EXAMPLES

- **Fake Login Pages**: Websites that look exactly like Microsoft 365 or Gmail but steal your credentials.

- **Invoice Scams**: Receiving an "Overdue Invoice" as a PDF attachment that contains malware.
- **Tech Support Scams**: A popup saying your computer is infected and giving a fake number to call.

## Best Practices for Prevention

- **Multi-Factor Authentication (MFA)**: Always enable MFA to provide an extra layer of security.
- **Think Before You Click**: Verify any suspicious request by contacting the sender through a known, official channel.
- **Keep Software Updated**: Ensure your browser and antivirus are always up to date to block known threats.
- **Report Suspicious Activity**: If you see something, notify your IT or security team immediately.

## Interactive Quiz (Spot the Phish)

1. **Question**: You receive an email from "IT Security" asking for your password to "verify your account." Do you give it?
    - *Answer*: No. Legitimate IT departments will never ask for your password.
2. **Question**: A link in an email leads to `www.google-security-update.net`. Is this safe?
    - *Answer*: No. The domain is not `google.com`; it is a fake site.