# Phishing Awareness Training

This playbook outlines the steps to educate employees about phishing scams, including recognition and prevention techniques, in order to safeguard corporate data.

### Step 1: Identify Audience

Determine which groups of employees will be participating in the training, focusing on those with access to sensitive information.

### Step 2: Develop Material

Create comprehensive educational material covering types of phishing scams, methods used by attackers, and case studies of phishing attacks.

### Step 3: Schedule Sessions

Organize training sessions at convenient times for all employees and ensure they are mandatory.

### Step 4: Conduct Training

Execute the training sessions, encouraging interaction and engagement from employees to maximize understanding and retention of information.

### Step 5: Evaluate Understanding

Assess the employees' understanding of phishing scams through quizzes or practical tests, to ensure the effectiveness of the training.

### Step 6: Provide Resources

Distribute additional learning resources, such as booklets or online materials, for further self-education and reference on phishing prevention.

### Step 7: Simulate Phishing

Run simulated phishing campaigns to provide a real-world experience and evaluate the employees' reactions to potential phishing attempts.

### Step 8: Gather Feedback

Collect feedback from participants to improve future training sessions and understand any remaining areas of confusion or concern.

### Step 9: Update Training

Regularly update training material to include new phishing techniques and ensure the information remains current and relevant.

## General Notes

### Continuous Learning

Phishing threats evolve continually; thus, education on the topic should be an ongoing process, not a one-time event.

### Encourage Reporting

Instill a culture where employees feel safe to report suspected phishing attempts without fear of reprisal or ridicule.

### Support System

Ensure there is a support system in place for employees who might fall victim to phishing, including an IT help desk and clear reporting processes.