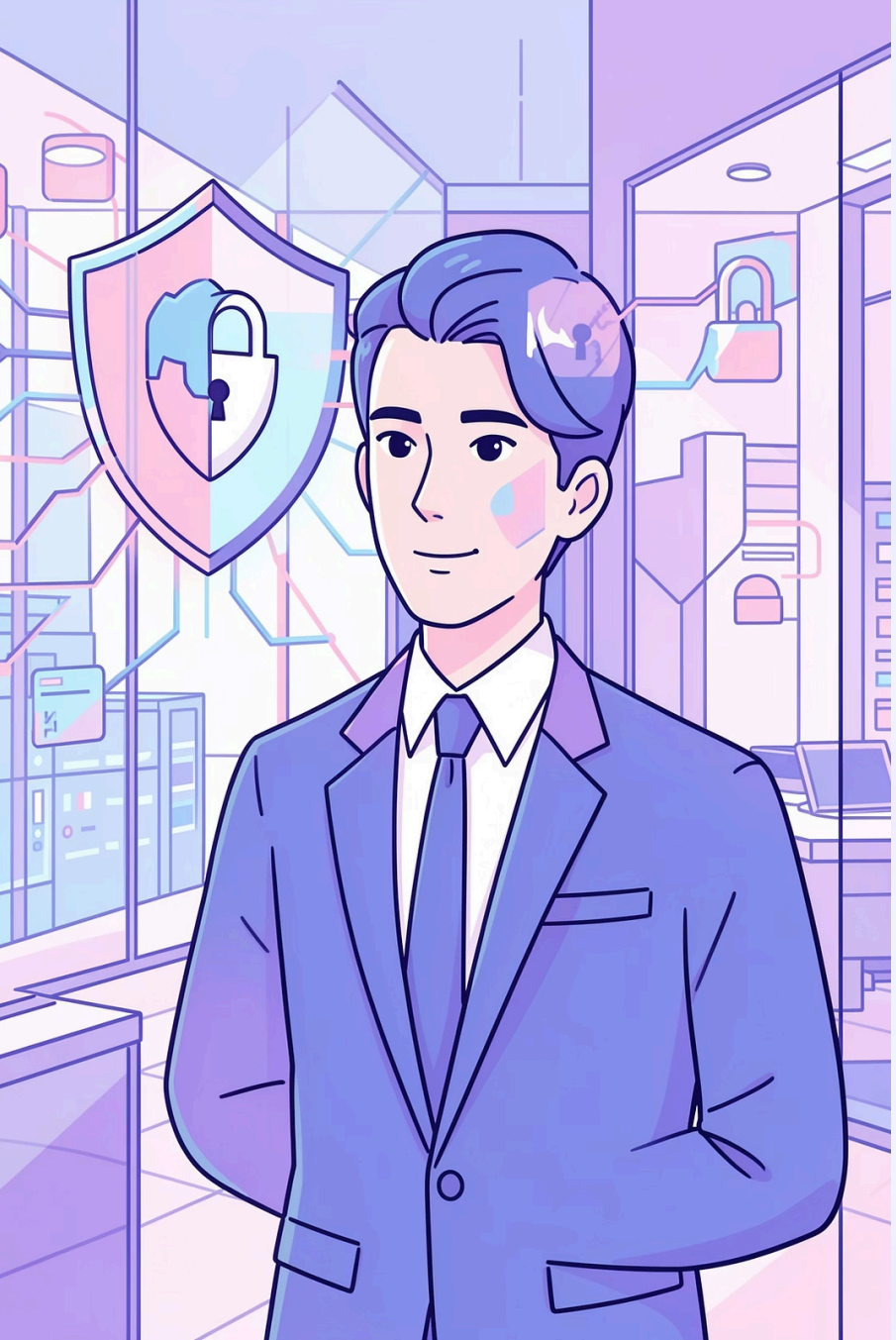


Social Engineering Defense

Security Awareness Training Design Project

Pretexting, Baiting, Tailgating & Psychological Manipulation

Prepared and Presented By:

- Shamanth R
- Madhurjya Deka
- Kacham Sai teja
- Ajith Mohan

| PG Certificate Program in AI/GenAI Powered Cybersecurity | 7 Feb 2026

Today's Roadmap

01

Training Needs Analysis

Assessing organizational security gaps and audience profiles

02

Module Design Document

Curriculum structure and learning outcomes

03

Assessment Strategy

Measuring knowledge and behavioral change

04

Engagement Techniques

Interactive scenarios and gamification

05

Implementation Plan

Rollout timeline and success metrics

06

Executive Summary

Program overview and ROI projections

Executive Summary

Purpose & Value of the Program

The Challenge

Social engineering drives 90% of security breaches

Technology alone cannot stop human-based attacks

Our Approach

Behavioral defense training, not just awareness

Role-based learning with real-world scenarios

Expected Outcomes

Reduced incident risk by 60%

Improved employee vigilance

Measurable security maturity growth

Why Social Engineering Works

Psychology Over Technology

Attackers Exploit Human Nature

Trust

We naturally want to help colleagues

Authority

We comply with perceived leadership

Fear

Threats trigger immediate action

Curiosity

Unknown links tempt exploration

Urgency

Time pressure bypasses critical thinking

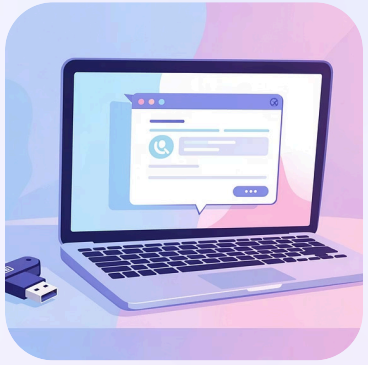
"Understanding attacker psychology is the first step to defense."

Common Social Engineering Techniques

The Attack Surface Overview

Pretexting

Fabricated scenarios to extract sensitive information



Baiting

Tempting offers that deliver malware or steal credentials

Tailgating

Physical security breach via social courtesy

Psychological Manipulation

Emotional triggers that bypass rational judgment

Pretexting & Baiting

Threat Deep Dive

Pretexting Tactics

Attackers create convincing false identities to justify requests

- Fake IT support calls
- Vendor impersonation
- Executive assistants requesting wire transfers
- Background verification "surveys"

Defense: Always verify identity through known channels

Baiting Exploits

Malicious lures that exploit curiosity and greed

- Infected USB drives in parking lots
- Free software downloads with malware
- "You won a prize" email links
- Fake job offers requiring credential submission

Defense: Adopt zero-trust mindset for unexpected offers

Tailgating & Psychological Manipulation

Physical + Emotional Exploitation

Tailgating Threats

Unauthorized physical access via social courtesy

- Following employees through secure doors
- Exploiting politeness and "helpfulness"
- Common in offices, data centers, server rooms

Psychological Manipulation Tactics

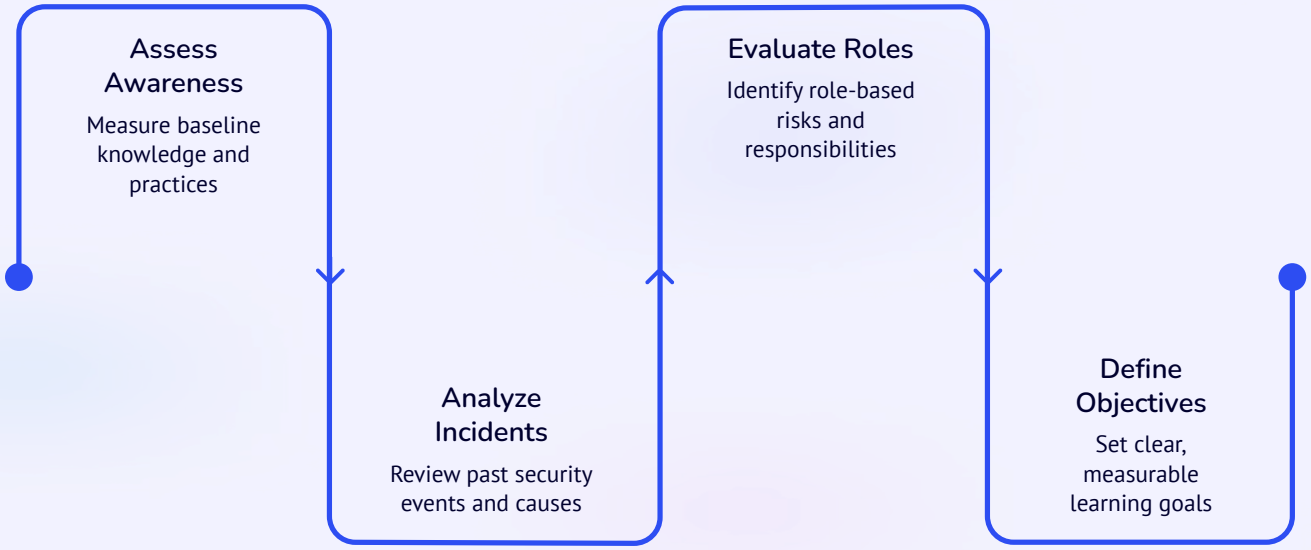
Emotional triggers that override security protocols

- **Fear:** "Your account has been compromised"
- **Authority:** "The CEO needs this immediately"
- **Urgency:** "You must act within 10 minutes"

Key Message: Humans are the primary attack vector. Technical defenses fail when people do.

Training Needs Analysis

Deliverable 1: Understanding the Audience



Assessment Areas
Target Audiences

- General employees (all departments)
- IT/Admin staff (elevated privileges)
- Executives (high-value targets)

Comprehensive evaluation identifies gaps and defines clear, measurable learning objectives per role

- **Current Awareness Level**

  Baseline knowledge and security practices

- **Past Incidents**

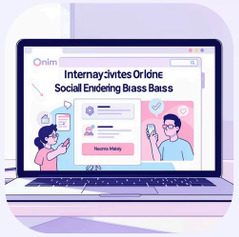
  Historical breaches and near misses

- **Role-Based Risk Exposure**

  Department-specific vulnerabilities

Module Design Document

Deliverable 2: Comprehensive Curriculum Structure



Module 1: Social Engineering Basics

Foundational concepts and attacker methodologies

Module 2: Pretexting Defense

Identity verification protocols and red flag recognition

Module 3: Baiting Defense

Zero-trust practices for unexpected offers and media

Module 4: Tailgating Prevention

Physical access control and challenge procedures

Module 5: Psychological Manipulation Awareness

Recognizing emotional triggers and pressure tactics

Delivery Methods

- Instructor-led workshops
- Scenario-based simulations
- Microlearning video modules
- Interactive e-learning platform

Assessment Strategy

Deliverable 3: Measuring Training Effectiveness

Assessment Components

1

Pre-Training Baseline Quiz

Establish initial knowledge levels

2

Post-Training Assessment

Measure knowledge acquisition

3

Scenario-Based Exercises

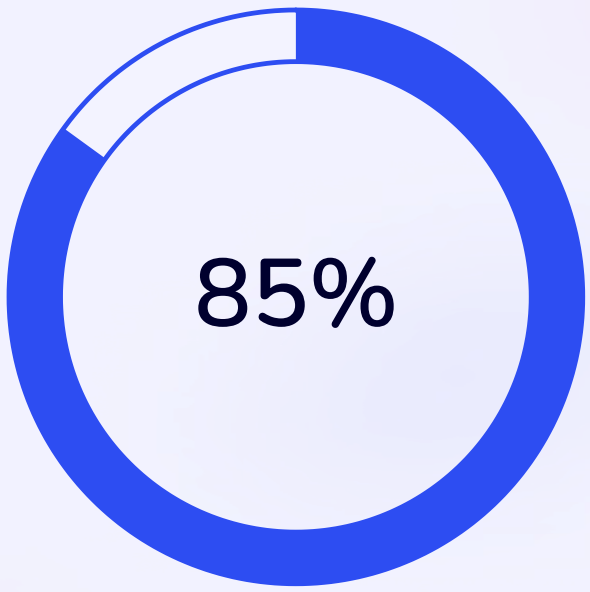
Real-world application testing

4

Behavioral Observation

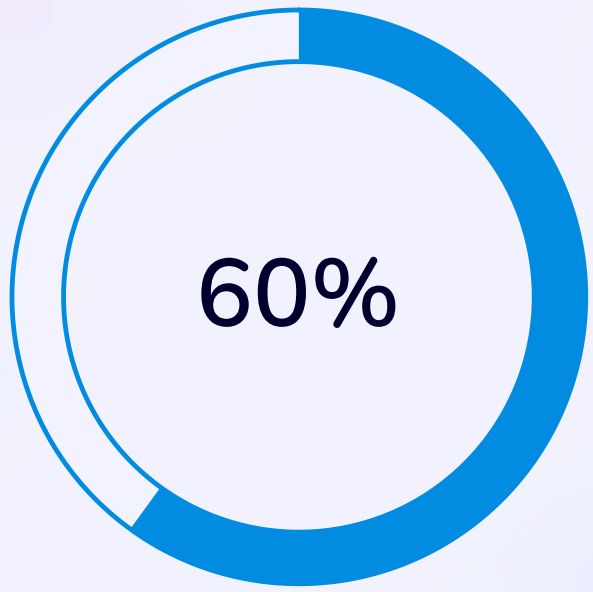
Ongoing monitoring and simulated attacks

Success Metrics



Knowledge Improvement Target

Average score increase post-training



Risk Behavior Reduction

Decrease in simulated attack success rate

Reporting Increase

Triple the incident reporting rate

Engagement Techniques

Deliverable 4: Keeping Learners Involved

Key Techniques

Gamified Quizzes

Interactive challenges to test knowledge.

Role-Play Simulations

Hands-on practice with social engineering scenarios.

Phishing & Baiting Scenarios

Simulated attacks to build recognition and response.

Leaderboards & Rewards

Encourages participation and healthy competition.

Why They Are Effective

Emotional Involvement

Strengthens memory and long-term retention.

Learning by Doing

Active participation solidifies understanding.

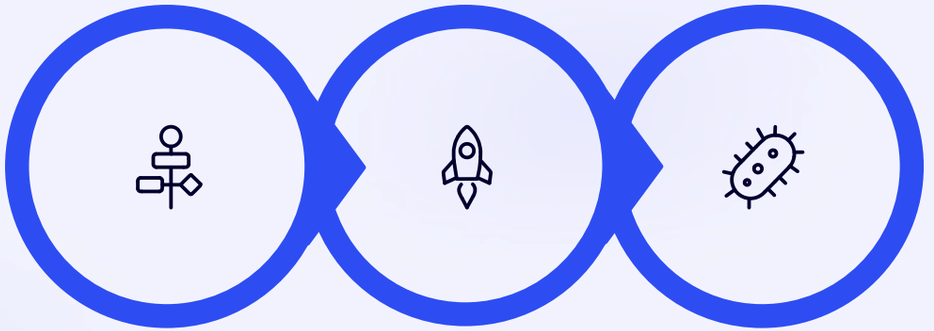
Behavioral Change

Repeated practice forms new, secure habits.

Implementation Plan

From Design to Deployment

Deployment Timeline



Key Resources

- Dedicated training team
- Leverage existing LMS platform
- IT security team for technical support
- Internal communications support

Success Metrics

A phased approach ensures smooth integration and minimal disruption across the organization.

Completion Rates

Target 95% across all employee groups

Assessment Scores

Average 80% post-training knowledge retention

Incident Reduction

Reduce social engineering incidents by 60%

Conclusion & Key Takeaways

Building a Human Firewall

Social engineering targets people, not systems

Human vulnerabilities are the weakest link in any security chain.

Awareness + practice = defense

Educated employees with practiced responses are the strongest defense.

Continuous training is essential

The threat landscape evolves, and so must our collective knowledge and skills.

"Security is not a tool — it’s a behavior."