# Designing Effective Phishing Awareness Training Using the ADDIE Model

A comprehensive framework for developing impactful security training that transforms employees into your first line of defense against cyber threats.

# Phase 1: Analysis – Understanding the Training Needs

### Target Learners

Employees across all departments with varying technical skill levels, from entry-level staff to senior executives

### Knowledge Gaps

Assess current phishing awareness, identify common vulnerabilities, and understand where employees struggle most

### Behavioral Outcomes

Define clear goals: recognize phishing attempts, report suspicious emails promptly, and avoid clicking malicious links

### Delivery Constraints

Account for remote workforce realities, diverse device usage, limited time availability, and varying internet connectivity

# Phase 2: Design – Blueprinting the Learning Experience

## Learning Architecture

Set **measurable learning objectives** aligned with organizational security goals and compliance requirements.

Develop comprehensive course outline covering:

- Types of phishing (email, SMS, social media)
- Red flag identification techniques
- Step-by-step reporting procedures
- Real-world case studies

## Instructional Strategies

Choose proven learning approaches:

- **Scenario-based learning** for contextual understanding
- **Microlearning modules** for busy schedules
- **Interactive quizzes** for knowledge retention
- **Spaced repetition** to reinforce key concepts

Plan engaging multimedia including animations, real phishing examples, and interactive simulations.

# Course Structure & Estimated Durations

| Module | Title | Format | Duration |
|---|---|---|---|
| 1 | Why Phishing Matters (context & impact) | Animation + real examples | 6 min |
| 2 | Phishing Red Flags (indicators) | Interactive checklist + hotspot activity | 10 min |
| 3 | Email Forensics (inspect headers, links) | Guided simulation (hover/inspect) | 12 min |
| 4 | Verification & Response Steps | Flowchart scenario + decision points | 10 min |
| 5 | Reporting & Company Policy | Walkthrough of reporting tool + video | 8 min |
| 6 | Quick tips, MFA, device hygiene | Quick tips, MFA, device hygiene | 6 min |
| 7 | Final Assessment & Certificate | 15 Q quiz (randomized) | 8-12 min |

Total learner core time: ~60 minutes (including assessment)

# Phase 3: Development – Creating Engaging Content & Tools

01

### Produce Digital Assets

Create compelling videos, clear infographics, and realistic phishing simulation exercises that mirror actual threats

02

### Build Interactive Modules

Design branching scenarios with decision points that mimic real phishing attempts and their consequences

03

### Collaborate with SMEs

Partner with cybersecurity subject matter experts to ensure technical accuracy, relevance, and alignment with current threat landscape

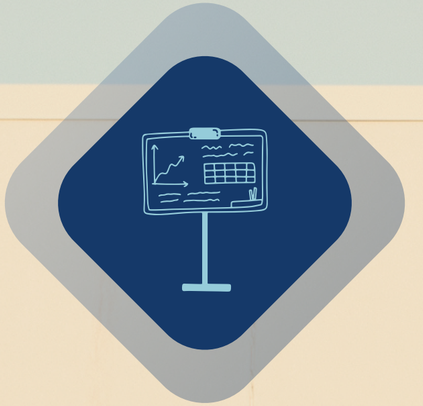
04

### Develop Assessments

Create knowledge checks, simulated phishing tests with immediate feedback, and comprehensive evaluation mechanisms

# Development

Tools and Outputs



### Storyboard Creation:

Detailed storyboards for videos and simulations

### Multimedia Production:

Professionally recorded voice-overs, animated graphics, and screen-casts showcase tool usage

### Programming:

SCORM-compliant modules developed in authoring tools (Adobe Captivate or iSpring)

### Assessment Items:

Multiple-choice quizzes, scenario-based decision making, knowledge checks

### Review:

Internal SME and user testing feedback incorporated for revisions


# Phase 4: Implementation – Delivering the Training Effectively

## Deployment

### Deploy via LMS

Launch training through a robust Learning Management System accessible on desktop, tablet, and mobile devices with seamless synchronization

## Simulation

### Flexible Scheduling

Offer both instructor-led webinars for real-time interaction and self-paced modules for individual learning preferences and time constraints

## Support

### Train Facilitators

Prepare instructors and support staff on course delivery, technical troubleshooting, and providing meaningful learner assistance

## Communication

### Launch Campaign

Communicate rollout plan through multiple channels, build excitement, and encourage active participation with compelling messaging

# Implementation

## Rollout Plan

- Weeks 0–1: Kickoff, align stakeholders, approve outline
- Weeks 2–4: Develop content (videos, quizzes, scenarios)
- Week 5: QA, accessibility check, LMS upload
- Week 6: Pilot with 30-40 users, collect feedback
- Week 7: Final edits, set simulation schedule
- Week 8: Full launch

## Phishing Simulation Plan

- Month 1: Baseline test (all users)
- Months 2–5: Monthly targeted simulations
- Month 6: Final simulation + performance review

1. **Types**: Fake logins, attachments, invoices, SMiShing
2. **Policy:** No punishment, retraining for clicks, HR notified only for repeated risks

## Communication Plan

- Pre-launch: Email from HR (2 weeks prior)
- Launch: LMS assignment + guides
- Reminders: At 7 days & 3 days pre-deadline
- Post-sim: Personalized feedback with learning tips

# Phase 5: Evaluation – Measuring Impact & Continuous Improvement

### Formative Evaluation

Conduct pilot testing during development with feedback loops to refine content before full launch

### Continuous Updates

Analyze results to identify gaps and regularly update content to address evolving phishing threats and tactics

### Summative Assessment

Measure post-training success through phishing simulation click rates, quiz scores, and behavioral change metrics

### Learner Satisfaction

Gather qualitative data via surveys, interviews, and focus groups to understand user experience

# Evaluation

## REPORTING CADENCE

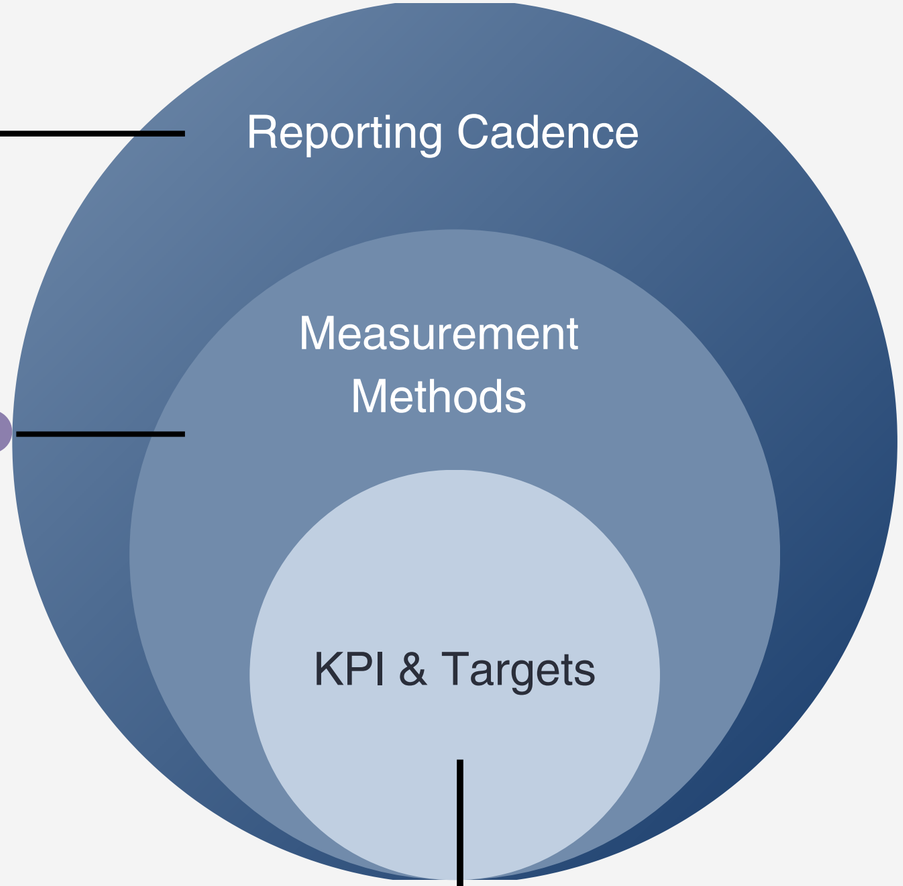
Weekly pilot reports
Monthly leadership dashboards
Quarterly business review

## MEASUREMENT METHODS

Reaction
Learning
Behavior
Results

## KPI & TARGETS

Course completion rate
Average quiz score
Phishing click rate
Report rate (reporting suspicious emails)



# Key Deliverables in the Design Document (DD)

### Course Design Blueprint

Detailed objectives, content mapping, learning pathways, and instructional strategies aligned with business goals.

### Implementation Plan

Detail the strategy for development & launch. Complete timelines, resource allocation, technical requirements, & multi-channel communication strategy

### Learner Analysis Report

Comprehensive needs assessment identifying skill gaps, demographics, and learning preferences

### Interactive Prototype

Storyboards & working prototypes, simulations, & assessments for stakeholder review & approval

### Evaluation Framework

Establish metrics to measure learning effectiveness through success, assessment, data collection,& reporting.

# Creative Elements to Enhance Engagement

## Case Studies

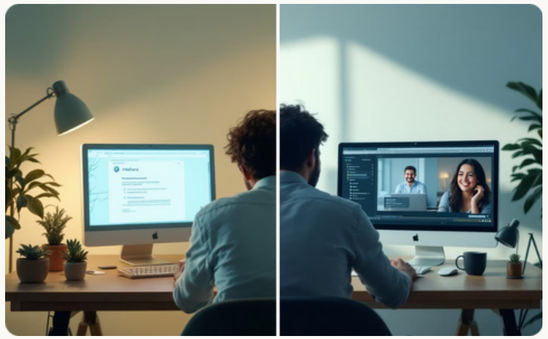
Feature actual phishing incidents with named companies, detailed attack vectors, financial impact, and lessons learned to create memorable learning moments

## Gamification

Introduce achievement badges, team leaderboards, recognition rewards, and friendly competition to motivate consistent phishing detection performance

## Positive Coaching Tone

Empower learners with encouraging language that builds confidence rather than using fear-based messaging that creates anxiety and resistance



## Visual Storytelling

Create compelling before-and-after scenarios demonstrating the tangible impact of phishing awareness on protecting personal and company data

# Appendices

## Resources

Subject Matter Experts, Multimedia Production Team, LMS Admin

## Timeline

12 weeks from analysis to launch

## Budget

Estimated costs for production licenses, personnel, & platform fees

## Risk & Mitigation

Technology issues, learner engagement challenges, planned contingency protocols.

# Execution Tips for Success

## Cross-Functional Collaboration

Involve IT security, HR, communications, and department leaders for a holistic, organization-wide approach

## Ongoing Refreshers

Schedule periodic refresher trainings quarterly and update simulations with emerging phishing trends and attack techniques

## Data-Driven Adaptation

Leverage LMS analytics to track learner progress, identify struggling areas, and adapt content for maximum effectiveness

## Security Culture Building

Foster continuous awareness through campaigns, newsletters, posters, and recognition programs that celebrate vigilant behavior

# Roles & Responsibilities

**Project Sponsor (CISO)**:
Executive support, policy approvals

**Project Manager**
Timeline, budget, stakeholder coordination

**Instructional Designer**
Learning objectives, storyboards, assessments

**Content Developer**
Build modules and produce media

**Security SME**
Technical review, simulation scenarios

**LMS Admin**
Upload packages, assign users, reporting

**Pilot Users**
Provide feedback on clarity and usability

**HR**
Policy alignment & approvals

# Building a Resilient Workforce

## Against Phishing Threats

### Systematic Approach

The ADDIE model ensures a rigorous, learner-centered methodology that produces measurable, lasting results

### Empowered Defenders

Well-structured phishing training transforms employees from vulnerabilities into active security defenders who protect organizational assets

### Continuous Excellence

Regular evaluation and iteration keep training relevant, effective, and aligned with the constantly evolving threat landscape

> **Together, we can transform phishing awareness from mere compliance checkbox to a thriving culture of cybersecurity vigilance and shared responsibility.**