Phishing Awareness Training

September 2024

Michelle Kauk

1. Introduction

This document outlines the design strategy for developing a phishing awareness training course for employees at a large insurance company. The course was built using the ADDIE model and will focus on scenario-based learning to enhance phishing detection skills. The training will be engaging, interactive, and accessible on desktop and laptop computers.

2. Key Problems

Phishing Threats: Employees regularly encounter phishing emails but struggle with identifying them consistently, leading to potential cybersecurity risks.

Inconsistent Application: Despite prior training, many employees fail to apply phishing prevention techniques in real scenarios, posing a security threat to the organization.

Time Constraints: Employees have limited time for training, so the course needs to be concise and flexible for busy schedules.

3. Audience Analysis

Primary Audience: Employees across various roles, including adjusters, underwriters, administrators, and support staff. They have varying levels of technical expertise and awareness of phishing tactics.

Demographics:

Age: 2560 years.

Education Level: High school diploma to college degree.

Technical Proficiency: Varies, with some employees being highly tech savvy while others have limited experience with digital tools.

Learning Preferences: Interactive and scenario-based learning with practical, role specific examples that can be applied in day-to-day tasks.

4. Current Knowledge and Skills

Awareness Level: Varies. Some employees are familiar with phishing tactics but often fail to apply their knowledge consistently, while others have minimal awareness.

Inconsistent Response: Even employees with awareness of phishing risks do not always follow best practices when responding to suspicious emails.

5. Key Challenges and Pain Points

Engagement: The course must be interactive and engaging to combat the perception that cybersecurity training is boring.

Time: Employees have limited time for training, so the course needs to be brief while still effective.

Technical Proficiency: The course must cater to a broad range of technical skills, ensuring that it is simple enough for less tech savvy employees but still valuable for more advanced users.

6. Training Gaps

Role Specific Scenarios: Current training lacks focus on the specific phishing threats employees in different roles face (e.g., underwriters vs. adjusters).

Lack of Engagement: Previous training approaches have been passive, leading to poor retention of knowledge and low application of phishing prevention techniques.

Behavioral Gaps: Employees do not consistently report suspicious emails, and many still fall victim to phishing scams.

7. Stakeholders and SMEs

Stakeholders:

- Company Executives (focus on cybersecurity protection)
- IT Security Team (oversee phishing detection and response)
- Human Resources (ensure training accessibility and completion)

Subject Matter Experts (SMEs):

- IT Security Personnel
- Learning and Development Team
- Compliance and Risk Management Experts

8. Learning Objectives

Knowledge:

1. Recognize common phishing email red flags, including suspicious links, sender addresses, and requests for sensitive information.
2. Understand the specific phishing threats relevant to different roles within the company.

Skills:

1. Correctly identify phishing attempts in real world scenarios.
2. Use company tools to report phishing emails promptly and effectively.

Attitudes:

1. Value the importance of phishing prevention and their role in protecting company data.
2. Commit to ongoing vigilance and continuous improvement in phishing detection.

9. Instructional Strategies

Design Approach:

ADDIE Model: Utilize the ADDIE framework (Analysis, Design, Development, Implementation, Evaluation) to ensure a structured and iterative course development process.

Scenario Based Learning: Use realistic phishing scenarios relevant to different job roles, with branching options to reinforce decision making.

Interactivity: Include knowledge checks, quizzes, and decision-making exercises to maintain engagement.

Multimedia Elements: Use a combination of graphics, videos (Vyond animation), and text to cater to different learning preferences.

Course Structure:

Introduction: Meet Alex, the course guide who will walk learners through the common phishing threats.

Module 1: Recognizing Phishing Emails (suspicious sender, generic greetings, etc.).

Module 2: Role Specific Phishing Threats (scenarios for adjusters, underwriters, administrators).

Module 3: How to Respond (reporting tools, IT support).

Knowledge Checks and Quizzes: Scenario based questions to test understanding.

Conclusion and Resources: Summary and quick reference guide download.

10. Evaluation

Formative Evaluation:

Pilot Testing: Run a small group pilot to ensure the scenarios are realistic and the course is engaging.

Feedback Mechanisms: Collect feedback from employees during and after the course to identify areas for improvement.

Summative Evaluation:

Completion Rates: Track course completion rates and time taken to complete the course.

Knowledge Retention: Evaluate employee performance on quizzes and knowledge checks.

Phishing Incident Tracking: Monitor changes in phishing reporting and clickthrough rates post training to assess long-term impact.

11. Conclusion

The phishing awareness training course is designed to address the unique cybersecurity challenges faced by employees in different roles within the company. By using scenario based learning and interactive exercises, the course will engage employees, helping them to retain key phishing detection techniques and apply them in their daily tasks. The course is structured to be brief yet impactful, ensuring that employees can complete it within a busy workday while gaining essential cybersecurity skills.