Think Before You Click: Spotting and Responding to Phishing Emails
Design Document

Project Overview

Scenario-based cybersecurity awareness microlearning course designed to help employees recognize phishing attempts and make safer decisions when interacting with email communications.

Business Need

Phishing attacks remain one of the most common cybersecurity threats facing organizations. Employees are frequently targeted through deceptive emails designed to steal credentials, install malware, or gain access to sensitive information.

Target Audience

Employees across all departments who use email and digital communication tools as part of their daily responsibilities.

Delivery Method

Self-paced microlearning, Articulate Rise 360, mobile-friendly design, approximately 5–7 minutes.

Learning Objectives

Recognize common phishing indicators; evaluate suspicious emails before responding; identify safe actions to take when receiving a phishing attempt; protect organizational data and systems.

Instructional Strategy

Scenario-based learning, decision-making practice, immediate feedback, performance support, retrieval practice, and authentic workplace contexts.

Course Structure

Introduction and objectives; phishing indicators; five workplace phishing scenarios; infographic reinforcement; key takeaways and course summary.

Assessment Strategy

Learners complete five scenario-based decision activities and receive immediate feedback explaining safe and unsafe responses.

Implementation

Designed for LMS deployment as part of cybersecurity awareness training or employee onboarding.

Evaluation

Measured through completion rates, learner feedback, scenario performance data, and phishing simulation results.