Design Document

Business Purpose	This module is a part of our multi-layered set of mitigations to help improve our company's protection against cyber threats. Phishing, a type of cyber attack, is currently our number one security risk and can be financially devastating to our company. We want to provide all of our employees who are vulnerable to such attacks the necessary information to be able to recognize and prevent the loss of sensitive information.
Target Audience	● All employees within the company's email domain
Knowledge Level	● Knowledge & Understanding
Training Time	● 30 minute seat time
Training Recommendation	This will be an interactive eLearning module for all employees that have a company email and can be potential victims of cyber security attacks. An eLearning course would allow our employees, who are spread across the US, to work through the content at their own pace and time. This module will focus specifically on the most common type of security threat called Phishing Attacks.

Deliverables	● Storyboard with narration script for voice-over
	● 1 eLearning course
	  ○ Developed in Articulate Storyline
	  ○ Includes voice-over AI narration
	  ○ Includes 3 learning sections
	    ■ What is Phishing
	    ■ Identifying a Phish
	    ■ Best Practices
	  ○ Quizzes
	    ■ 1 Knowledge Check
	    ■ Final Quiz
	● Resource linked on Module
	  ○ [Stay Safe From Cyber Attacks Infographic](#)
	    ■ This resource will also be utilized as a job aid and posted around in-person office spaces.

Learning Objectives	By the end of this module, the learners will be able to: 1. Classify types of phishing attacks. 2. Analyze potential security threats. 3. Identify best practices for preventing malware.

Training Outline	● Welcome
	● Navigation
	● Objectives
	● What is Phishing?
	  ○ Types of Phishing Attacks
	    ■ Explanation all 5 types of phishing attacks including spear phishing, smishing, vishing, clone phishing, and whaling.

Design Document

- ○ Successful Attacks
    - ■ Include ways that companies and individuals can be affected by an attack; identity theft, malware/ransomware installation, loss of sensitive information, data sold to criminals, financial loss, ans access to company systems
  - ○ Knowledge Check
    - ■ Covers Objective #1

- ● Identify a Phish
  - ○ This section will include scenario-based learning giving the learners examples of emails and texts that they might receive on their company account.
    - ■ Mismatched URLs
      - ● Example email from a fake company and a gif that shows how to view a url before clicking
    - ■ Poor Grammar/Spelling
      - ● Example email from a fake company that uses several grammar and spelling mistakes
    - ■ Unofficial Contact
      - ● Example text message from an unknown source about information that was no solicited
    - ■ Urgent Language
      - ● Example text message that tries to get the recipient to do something immediately
- ● Best Practices
  - ○ Give examples on all the ways to spot a potential threat and how to avoid them
    - ■ Email Address: looking at the end email, not just the sender
    - ■ Online Posts: Don't give away too much information
    - ■ Passwords: Create strong passwords
    - ■ Attachments; Never click on links or open attachments
    - ■ Domain: Check the domain in their email address first
- ● Quiz
  - ○ Five questions that match the learning objectives. Includes real life scenarios.
  - ○ Covers Objectives 1-3
- ● Summary
- ● Congratulations

Assessment Plan	80% passing on eLearning assessment of 5 questions ● Mixture of multiple choice and scenario-based questions to address learning objectives. ● Knowledge Checks not included in score quiz score.

Evaluation of Success	- Decreased Phish-Prone percentage on Phishing Security Test Results - Increase company benchmark compared to others in industry