Email Security 101: Design Document

Business Purpose	The Email 101 Course is designed as a one-year refresher training on identifying the most common types of email security threats, seeing real life examples in practice, and learning the implications of falling victim to these attacks. The learners have already gone through an extended training on keeping private and sensitive company information safe upon orientation to their specific roles in their first week of employment. This course is designed to refresh staff on the topic after one year, and keep compliance rates in check, with a 90% compliance rate to follow email protocols and report suspicious email activity.
Target Audience	All 200 employees
Training Time	20 minutes
Training Recommendation	E-learning course: An e-learning course was selected for this topic due to the large nature of the audience, all with various specific roles. This course is designed as a general refresher, as all staff have gone through detailed and specific security training within their department and role. • The information will be scaffolded throughout the course, where the learner is first introduced to the negative implications and common types of threats, but will later practice as they view real-life email scenarios to learn the negative implications of poor email security. • The course will begin with a phone recording of an individual calling IT to ask for help after clicking an email she later realized was suspicious. • This will lead to a pre-knowledge check to test the learners knowledge on what email activity the woman fell victim to. • Throughout the course the learner will be introduced to the most common types of email threats and how they can negatively impact a recipient if opened, clicked, or downloaded. • The learner will examine real-life emails to see what each type of attack looks like in the real world and see the implications of falling victim to these email attacks. • The course will end with a final assessment.
Deliverables	The delivery will be created through Storyline 360 and will include: • Story board and script prior to development. • Narration using Wellsaid Labs. There is no dialogue, so only one VO is required; please use Jeremy G. as the VO. • Images of real-life email examples of the various types of email security threats. • Final Graded Assessments.

Learning Objectives

After completing this course, the learner will be able to:

- Identify the most common types of email attacks and their risks
- Recognize the various types of PI and how to safeguard this information daily
- Identify suspicious email activity to report

Training Outline

Introduction

- Pre-course scenario and knowledge check with phone recording of an email security attack gone wrong. The learner will re-acquaint themselves with the topic by selecting the type of attack the victim fell prey to. This will allow the learner to recall information previously learned in their employee orientation.

Module 2: The importance of internet Security

- In this module the learner will be reminded of the negative implications of practicing poor email security both at work and in their personal life, and will recognize the importance of practicing proper email security.
    - Animated slides will provide information on screen about the importance of email security and social engineering. Interactive slide will allow learners to click various images to identify:
      1.) The types of Personal Information

      2.) How Personal Information can be accessed with poor storage of personal information

      3.) How proprietary information can be stolen from this stolen data.

Module 3: Common Email Threats

- In this module the learner will review the most common types of email threats. An email box will appear with the types of threats displayed as the email subjects for learners to click, see examples of the type of email threat while voice over defines the type of email threat.
- An accordion slide will display more in-depth phishing threats that were introduced in the previous slide. Learner will click on 3 tabs to learn about deception phishing, spear phishing, and whaling.
- Next, the learner will be introduced to interactive examples of real-life emails to learn the negative implications of clicking, downloading, or following the directions in email attacks. The learner will see an email example and prompted to “click” “download” or follow some form of instruction on the email, which will lead them to a layer describing the mistake that was made and the negative implications.

	Module 4: The learner will explore best practices to follow for keeping emails safe and secure. These are the practices that staff are expected to follow for keeping email information safe. Introduction to Assessment Assessment Summary/ Conclusion: User will revisit the Learning objectives and will have the opportunity to exit the course after passing the final assessment.
Assessment Plan	• Learner will answer 5 questions, with an 80% needed to pass the final assessment and complete the course. • Multiple Choice assessment questions will quiz the learner on identifying best practices and ensure staff can identify the most common email attacks and how to avoid them. • Responses will be shuffled, and if the learner does not pass they will have the opportunity to review before continuing and re-taking the final assessment. • Learner can re-take the final assessment as many times as needed until passing percentage is acquired.