Design Document

Training Title: Email Security for Employees

Business Goal and Problem	- Safe & Sound Insurance's main goal is **building and maintaining trust** with each client through a focus on **protecting confidential client information** by **increasing email security**. - The IT department can only put so many filters in place; some deceptive phishing emails will make it to the inboxes of employees leaving Safe & Sound and its clients vulnerable. However, many employees are unaware of the dangers of such email scams or what to look for to identify them. It is necessary to explicitly teach employees how to properly secure their email accounts to protect clients and the business.
Target Audience	- All current Safe & Sound Insurance **employees**, and new hires from here on. - This will include a range of ages and computer expertise. However, all employees should have basic (entry-level) knowledge of and be able to use a computer and email account. - Current employees will already have passwords set up for their email accounts, but they may need to be updated after the training
Learning Objectives	**Terminal LOs:** By the end of the course, employees will be able to 1. Create a strong password. 2. Identify phishing email scams 3. Properly handle/respond to phishing emails **Enabling LOs:** 1. Explain the vital role of email security in safeguarding client information. 2. Identify the 3 criteria for a strong password.
Training Recommendation	**Delivery Method:** - Articulate Storyline e-Learning course **Approach:** - Continuous workplace scenario (customer concern about data breaches leads one employee to getting help from IT)
Training Time	20 minutes of seat time

Deliverables	- Published SCORM zip files - eLearning module developed in Storyline 360 with Voiceover Narration - Storyline 360 source file (.story file) - Storyboard, including script
Training Outline	1. Introduction to Course a. Navigation Tutorial b. Learning Objectives 2. Importance of Email Security a. Begin Workplace Scenario with Daniel (employee) and Ava (IT) i. Daniel is unsure what his role is in email security or why it matters ii. He asks Ava from IT for help b. Interaction- data breach stats c. Knowledge Check 1 3. How to Secure Your Email a. Password Security b. 3 criterion of a strong password i. Easy to remember, yet difficult to guess ii. Avoids common phrases, and is completely original iii. Should be at least 8 characters mixed w/ numbers, symbols and caps/lower case c. Knowledge check 2 4. Phishing Email Awareness a. The basics: i. What is a phishing email ii. What it aims to do iii. How to identify one 1. Typos/weird formatting 2. Sender name does not match business or organization email is from 3. Attachments or links to open b. How to Identify i. 3 actual phishing email examples to look at ii. Markers/ red flags to identify the signs iii. Knowledge Check 5. How to handle phishing emails a. Accordion interaction of what to do/not do i. Do not open any suspicious emails ii. Never click open any links or attachments iii. Never provide any personal info iv. Report to IT dept. 6. Summary 7. Final Graded Quiz
Assessment	**Level 2 Assessment:**

Plan	- Knowledge Checks throughout - LO1- check understanding of the criteria for a strong password so they will be able to determine if a password is strong - LO2- check understanding of what to look for to identify a phishing email in their inbox before moving on to how to handle one - **Performance-based Final Graded Quiz** - Workplace scenario-based questions - 5 questions total (various question types) - 80% passing (4/5 correct) **Level 3 Assessment:** IT Dept. reports show - an **increase of employees reporting potential phishing scams** - **a decrease in phishing emails being opened** - Customer survey shows high ratings of trust and safety - Employees are observed easing customer minds by explaining our email security to them - Zero data breaches via phishing scams since training