Instructional Design Storyboard				
Scene	**Slide**	**Story**	**Text to be Included**	**Visual Descriptions**
1: Introduction	**1.1**	Alex, a newly promoted senior claims adjuster, is aware of increasing phishing threats and needs to complete the Phishing Awareness Training.	"Welcome to the Phishing Awareness Training. As a senior claims adjuster, it's crucial to stay vigilant against phishing threats."	A dashboard with a "Start Course" button. Introduce
	1.2	Alex logs into the e-learning portal to start the training.	"Let's get started!"	Alex's avatar sitting at a desk, logging into a computer.
2: Recognizing Phishing Emails	**2.1**	Alex learns about common phishing red flags.	"Phishing emails often contain generic greetings, suspicious links, and requests for sensitive information."	Examples of phishing emails with highlighted red flags.
	2.2	Alex receives an email from a client requesting an urgent change to a claim. The email looks suspicious.	"Urgent: Please update the claim immediately. Click the link below."	A simulated email with a generic greeting, suspicious link, and urgent language.
	2.3	**Branching Scenario:** Alex can choose to click the link or inspect it first.	Option A: Click the link. Option B: Hover over the link to inspect it.	Visual options with clickable buttons.
		Outcome of Branching: Depending on Alex's	Option A: "This link leads to a phishing website!"	Warning message for Option A:

	2.4	Depending on Alex's choice, the outcome is shown.	Option B: "Good job! You identified the phishing attempt."	Warning message for Option A; Success message for Option B.
	2.5	**Knowledge Check:** What are the red flags in this email?	"Which of the following is a red flag in the email Alex received?" A) Generic greeting B) Urgent language C) Request for sensitive information D) All of the above	Interactive multiple-choice question.
3: Role-Specific Red Flags	**3.1**	Different roles face different phishing threats. Alex reviews an email from "IT" asking for a password reset.	"Dear Alex, Please reset your password using the link below to maintain access to the claims portal."	A simulated email with spelling errors and an unfamiliar sender address.
	3.2	**Branching Scenario:** Alex can choose to reset the password or forward the email to IT.	Option A: Reset password. Option B: Forward the email to IT.	Visual options with clickable buttons.
	3.3	**Outcome of Branching:** Depending on Alex's choice, the outcome is shown.	Option A: "The portal is compromised!" Option B: "Good job! IT confirmed this was phishing."	Warning message for Option A; Success message for Option B.

	3.4	**Knowledge Check:** What should Alex do if they receive a suspicious email from IT?	"What is the best course of action if you receive a suspicious email from IT?"	Interactive multiple-choice question.
			A) Reset password	
			B) Ignore	
			C) Forward to IT	
			D) Reply for clarification	
4: How to Respond to Phishing Emails	**4.1**	Alex learns how to properly respond to phishing emails.	"Always report suspicious emails before taking any further action."	A checklist for handling phishing emails.
	4.2	Alex receives an email with an unusual attachment from a known client.	"Subject: Urgent - Please review attached document."	A simulated email with an unusual attachment and suspicious language.
	4.3	**Branching Scenario:** Alex can open the attachment or report the email.	Option A: Open the attachment.	Visual options with clickable buttons.
			Option B: Use the "Report Phishing" button.	
	4.4	**Outcome of Branching:** Depending on Alex's choice, the outcome is shown.	Option A: "The attachment contains malware!"	Warning message for Option A; Success message for Option B.
			Option B: "Good job! You correctly reported the phishing email."	
	4.5	**Knowledge Check:** What should Alex do first if they	"What should be your first step if you suspect an email is a phishing attempt?"	Interactive multiple-choice

	4.5	suspect an email is phishing?	A) Open attachment B) Reply for clarification C) Report phishing D) Delete immediately	question.
5: Company Resources and Support	**5.1**	Alex is reminded of company resources to deal with phishing threats.	"Remember to use company resources if you're ever unsure about an email."	Icons representing IT Helpdesk, Reporting Tools, and Training Resources.
	5.2	Alex encounters an unfamiliar phishing email and considers reaching out for help.	"This email doesn't match any typical phishing patterns. What should I do?"	A simulated email that looks suspicious but not immediately recognizable as phishing.
	5.3	**Branching Scenario:** Alex can delete the email or contact IT Helpdesk.	Option A: Delete the email. Option B: Contact IT Helpdesk.	Visual options with clickable buttons.
	5.4	**Outcome of Branching:** Depending on Alex's choice, the outcome is shown.	Option A: "The potential threat is not reported!" Option B: "Good job! IT helped identify the phishing attempt."	Warning message for Option A; Success message for Option B.
	5.5	**Knowledge Check:** What should Alex do if unsure about an email?	"What is the best action if you're unsure whether an email is phishing?" A) Delete it without reporting B) Contact IT Helpdesk C) Reply asking if it's legitimate D) Forward it to a colleague	Interactive multiple-choice question.

6: Conclusion	**6.1**	Alex completes the training and feels confident in identifying phishing threats.	"Congratulations! You've completed the Phishing Awareness Training."	A congratulatory screen with a downloadable "Phishing Awareness Quick Reference Guide."
	6.2	Alex is encouraged to participate in future phishing simulations.	"Stay sharp! Keep practicing your phishing detection skills."	A visual invitation to participate in future training or simulations.
	6.3	**Final Knowledge Check:** A comprehensive scenario where Alex must identify phishing red flags and choose the correct response.	"Final Challenge: Identify the phishing red flags and choose the correct response."	An email with multiple red flags and branching options for actions.