Design Document

Training Title: Open Roads' Gone Phishing Course

Business Goal and Problem	Success for Open Roads Insurance is to reduce the amount of malware found on computers within the claims department from 33% to 10%. Many of the claims agents in the call center are new to the workforce. They are having difficulty correctly identifying phishing attempts and are left susceptible to malware attacks. After this training, the claims agents will be able to identify 90% of phishing emails and report them appropriately.
Target Audience	This training is for the call center agents with Open Roads Ins. Most of these representatives are new to the workforce, in their early to mid twenties so they are unfamiliar with cyber attacks and phishing attempts. They work directly with the public, receiving both calls and emails from customers. Some of these emails have pictures or other media attached to them, and the representatives need to be able to distinguish between real emails/attachments and phishing attempts.
Learning Objectives	**Terminal LOs:** 1. Differentiate between a valid email and a phishing email. 2. Recognize the validity of email attachments. 3. Judge the validity of links found within emails. **Enabling LOs:** 1. Identify red flags of phishing emails. 2. Recognize emails sent from legitimate clients who are sending pictures or other attachments that were requested for their claim. 3. Recognize some of the differences between a valid link in an email and a phishing link.
Training Recommendation	**Delivery Method:** eLearning created in Storyline Job Aid showing employees how to set up Spam filters on their own in Chrome to ensure they are better protected in the online space **Approach:** Narrator (Ahab) leads you through a series of mini scenario based training with real-world examples
Training Time	This training should take about 15-20 minutes to complete.
Deliverables	eLearning module with VO developed in Articulate Storyline

	SCORM file for LMS eLearning module .story file Storyboard with script Spam filter job aid

Training Outline	• Intro to course
	• Navigation
	• Learning Objectives
	• Quick definition of Phishing
	  ○ Definition of Sensitive Data
	  ■ Passwords
	  ■ Credit Card Info
	  ■ Company Info
	  ■ Can result in Identity Theft or Financial Loss
	• Types of Phishing Emails
	  ○ Spam Email
	  ○ Spear Phishing
	  ○ Link Manipulation
	  ○ Malware
	• Knowledge Check
	  ○ Recognize the different types of Phishing Emails
	• Common attributes of Phishing Emails
	  ○ Too Good to be True
	  ○ Sense of Urgency
	  ○ Unusual Sender
	  ○ Hyperlinks
	  ○ Attachments
	• Red Flags found in Emails
	  ○ Sender/Receiver
	  ○ Date & Time
	  ○ Attachments
	  ○ Grammatical errors in body text
	  ○ Links
	• Knowledge Check
	  ○ Click on the Red Flags (Herrings)
	• How to Protect Self and Company from Phishers
	  ○ Spam Filters
	  ○ Browser Settings
	  ○ Monitoring Systems
	  ○ Email Links
	• Assessment with 5 questions
	• Conclusion & Congratulations

Assessment Plan	**Level 2 Assessment:** Two ungraded Knowledge Checks. The first one is after Types of Phishing Emails to ensure learners can recognize the differences between **Spam Email, Spear Phishing, Link Manipulation,** and **Malware**. The second Knowledge Check is after Red Flags to give learners a chance to locate the various red flags in example emails on their own. There will be 5 graded scenario based questions at the end of the training. Each question will assess a different aspect of common phishing attempts to ensure the learner knows what or where to check for suspicious emails, attachments, and links. **Level 3 Assessment:** Send out fake phishing emails, four per month, but vary the time in between each test, to ensure employees are reporting them as spam. If employees fail these random tests twice within a calendar month, they will need to retake the training.