Design Document

Training Title: Cyber Security Training

Business Goal and Problem	Employees lack a comprehensive understanding of cybersecurity best practices, leaving the organization vulnerable to cyber threats such as phishing emails, weak passwords, and scam websites. This knowledge gap has led to repeated security breaches, putting sensitive employee and customer data at risk. These incidents have not only compromised valuable data but have also resulted in significant financial and time costs for remediation. Without a more robust, ongoing training program that addresses these vulnerabilities, the company will continue to face costly security breaches, putting both its reputation and operations in jeopardy. Closing this gap by providing deeper cybersecurity education will help mitigate these risks and enable the organization to reach its goal of improving overall cybersecurity awareness and reducing incidents. Successful outcomes will include a 90% employee completion rate for training, a 50% improvement in cybersecurity knowledge based on post-training assessments, and a 30% reduction in security incidents due to better employee adherence to best practices. Additionally, clients will report a 95% satisfaction rate, with increased confidence in their organization's cybersecurity readiness and a desire for continued training.
Target Audience	All employees of multiple genders. The age range of the employees ranges approximately from 23 - 60. These employees have a foundational understanding of basic cybersecurity practices, such as password protection and recognizing phishing emails.
Learning Objectives	**Terminal LOs:** ● Create stronger passwords. ● Identify phishing emails. ● Recognize suspicious websites. ● Encrypt emails and other such materials that contain sensitive and private data. **Enabling LOs:** ● Utilize strong password practices when creating new passwords. (length, complexity, and randomness) ● Recognize common characteristics of phishing emails (e.g., unfamiliar senders, spelling errors, urgent language) ● Identify insecure websites, and how to protect personal and company data while browsing.
Training Recommendation	**Delivery Method:**

	● E-Learning ● Articulate Storyline 360 **Approach:** ● Mini-Scenarios ● Ungraded Knowledge Checks ● Performance Based Assessment
Training Time	20 minutes
Deliverables	● CyberSecurity.story ● Cybersecurity.zip ● Storyboard ● Voiceover Script (Separate document)
Training Outline	**1. Title Screen** a. Home Slide b. Navigation Page c. Overview d. Learning Objectives e. Menu **2. Password Protection** a. Password Strength Intro b. Mini Scenario c. Strong vs. Weak Passwords d. 2 Factor Authentication (2FA) e. Password Strength Ungraded Knowledge Check **3. Phishing** a. Phishing Intro b. Mini Scenario c. Phishing Statistics d. Handling Phishing Attempts e. Spotting Phishing Emails f. Phishing Ungraded Knowledge Check **4. Safe Internet Browsing** a. Safe Browsing Intro b. Mini Scenario c. Safe and Unsafe Websites

	d. Public Wi-Fi and VPN's (Virtual Private Network) e. Safe Internet Browsing Ungraded Knowledge Check **5. Data Protection and Disposal** a. Data Protection and Disposal Intro b. Mini Scenario c. Encryption Techniques (Symmetric) d. Encryption Techniques (Asymmetric) e. Secure Data Sharing Methods f. Data Disposal g. Data Privacy Laws h. Data Protection and Disposal Ungraded Knowledge Check **6. Assessment** a. Assessment Intro b. Password Assessment Question c. Phishing Assessment Question d. Browsing Assessment Question e. Data Protection and Disposal Assessment Question f. Wrap Up
Assessment Plan	**Level 2 Assessment:** ● Each section of the training contains 1 Knowledge Check. ● 4 Scenario based questions based on information covered in each section. The learner will need to achieve 75% to pass the assessment. **Level 3 Assessment:** ● 3 month post training observation of employee utilizing stronger passwords, recognition of unsafe websites and emails, as well as practicing proper data protection and disposal ● Manager interview regarding status of financial losses due to compromised data and security breaches.