Crystal Silva -
Barrios



CyberSmart

CYBERSECURITY AWARENESS FOR CORPORATE TEAMS

PROJECT DESCRIPTION

- **Program Name:** CyberSmart: Cybersecurity Awareness Training
- **Type of Program:** Corporate Digital Safety Training
- **Organization Type:** Corporate/Administrative
- **Program Participants:** All corporate employees with access to digital systems
- **Program Length:** 3 weeks (self-paced modules with live kickoff and wrap-up sessions)
- **Program Location:** Online LMS and virtual simulation platform





LEARNING THEORY

COGNITIVISM + BEHAVIORISM

Cognitivism focuses on how learners process, organize, and retain information.

- This theory guided the design of chunked, scenario-based lessons, where cybersecurity content is broken down into manageable modules.
- It supports the use of visuals, real-world examples, and guided reflection to help employees make meaningful connections between what they learn and how it applies to their work.

Behaviorism emphasizes learning through observable behavior changes, reinforced by stimuli and feedback.

- In this program, behaviorism shows up through interactive simulations, quizzes with instant feedback, and gamified activities that reward correct security actions.
- Learners are encouraged to practice safe behaviors repeatedly until they become habits—like spotting phishing emails or securing sensitive data.

By blending these two theories, the program ensures that employees are not only informed about cybersecurity, but are also motivated and trained to act on that knowledge consistently in their everyday tasks.

PROGRAM GOALS & OBJECTIVES

GOAL 1: IMPROVE AWARENESS OF CYBERSECURITY THREATS WITHIN THE FIRST WEEK OF TRAINING.

- Objective: By the end of Week 1, participants will be able to identify at least 5 common cybersecurity threats, including phishing, malware, and social engineering, with 80% accuracy on a knowledge quiz.

GOAL 2: INCREASE CORRECT APPLICATION OF CYBERSECURITY PRACTICES BY THE END OF WEEK 2.

- Objective: Participants will apply company-approved password management and data handling protocols in two interactive eLearning activities and receive a score of 80% or higher on performance tasks.

GOAL 3: STRENGTHEN SECURE DIGITAL BEHAVIOR THROUGH SIMULATION PRACTICE BY THE END OF THE COURSE.

- Objective: In the final week, participants will respond to 3 simulated cyber incidents using proper procedures and decision-making strategies, achieving a minimum of 3 out of 4 on the scenario performance rubric.







LEARNING OBJECTIVES

- By the end of the training session, learners will be able to identify at least three characteristics of weak vs. strong passwords and construct a secure password that meets company security standards with 100% accuracy in a hands-on activity.
- Within the 30-minute phishing simulation, learners will apply email safety protocols to distinguish between legitimate and suspicious emails, correctly identifying at least 4 out of 5 phishing or spoofing attempts.
- After completing the interactive module, learners will demonstrate secure file-sharing and document handling practices by scoring at least 80% on a practical assessment that includes real-world file-sharing scenarios.
- By the end of the final scenario-based activity, learners will evaluate cybersecurity risks in two simulated workplace situations and propose one appropriate mitigation strategy per scenario, receiving instructor feedback for accuracy and effectiveness.

INSTRUCTIONAL PLAN

Learning Objective	Group/ Individual Technique	Method of Facilitation
Apply email safety protocols	Individual Activity	Learners complete an interactive eLearning module with branching scenarios, identifying phishing emails. Instant feedback reinforces correct identification and explains incorrect choices.
Demonstrate secure file handling practices	Small group case study	In peer discussion forums, learners review realistic data mishandling scenarios, discuss consequences, and propose solutions. A facilitator guides with feedback.
Recognize weak vs. strong passwords	Individual Gamified challenge	Learners engage in a drag-and-drop exercise to build secure passwords from given word banks, earning badges for accuracy and speed.
Evaluate risks in digital workplace scenarios	Individual & group simulation + debrief	Participants complete a simulation-based assessment (e.g., phishing attack response) and then attend a group debrief session to reflect on decision-making and real-world implications.

TRANSFER OF LEARNING PLANNING

Purpose of Evaluation:

To measure the effectiveness of the training in reducing risky digital behaviors and incr
cybersecurity compliance.

Use of Results:

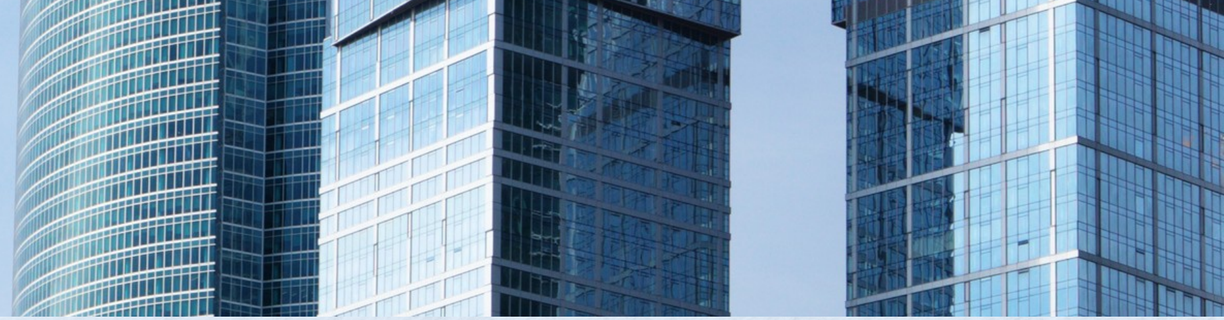
- Inform HR and IT on knowledge gaps
- Guide future cybersecurity initiatives
- Adjust and improve content delivery and simulation design



EVALUATION PLAN

Technique	Type	Description	Success Criteria
Pre/Post Quiz	Quantitative	Multiple-choice questions to assess baseline vs. final knowledge	Score improvement of 20%+
Scenario Performance Rubric	Qualitative	Rubric evaluating decision-making in simulations	80%+ mastery on rubric
Feedback Survey	Qualitative	Anonymous learner feedback on training effectiveness	85% satisfaction rate



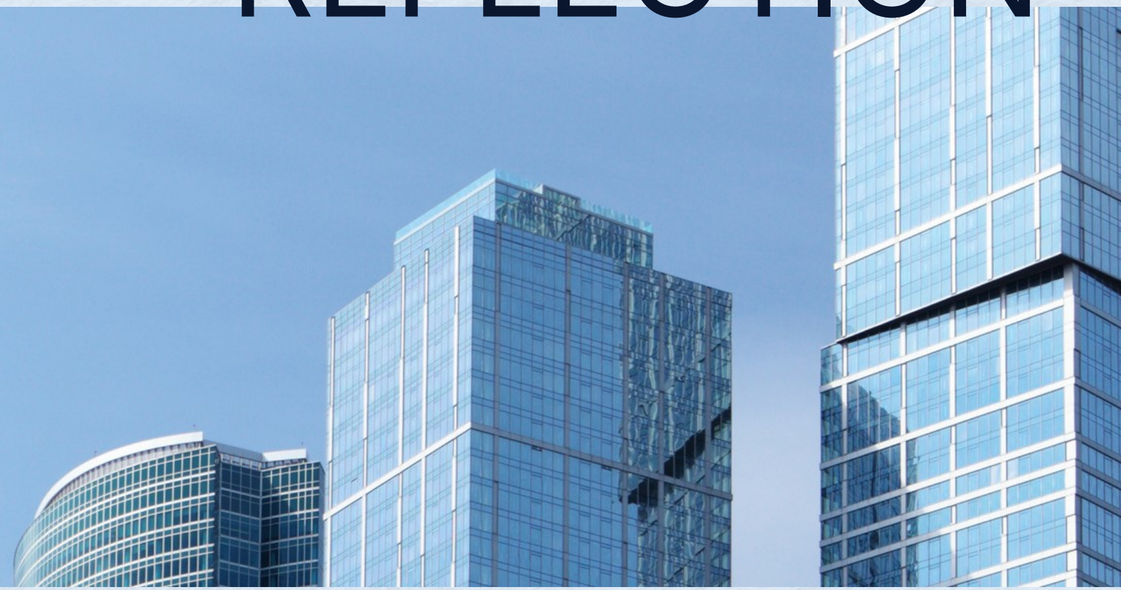


TECHNIQUES FOR COLLECTING DATA

Collection Tool Example:
Scenario Performance Rubric

- Criteria: Appropriate response, reasoning, outcome awareness
- Scale: 1–4 (Needs Improvement to Exceeds Expectations)
- Example item: “Correctly identifies phishing signs and reports to IT support”

PERSONAL REFLECTION



The most important part of the planning process was the Needs Analysis. It uncovered critical internal data such as phishing incidents and audit reports that shaped the goals and instructional design of the program. Understanding what the learners needed allowed me to tailor an effective, relevant, and action oriented learning experience.

THANK YOU

