Designing a Security Awareness Plan

This document outlines a structured approach to creating a customized security awareness plan aimed at changing employee behavior. The goal is to produce a clear, written plan that moves beyond simple compliance and focuses on measurable results.

Phase 1: Brainstorming

Begin by identifying one common, risky employee behavior you observe most often. This initial brainstorming task sets the foundation for the entire plan.

Phase 2: Identifying Training Gaps

Select a single risky behavior to focus on. Discuss and complete a

Risk → Training Need table. This process helps you pinpoint the root cause of the behavior and determine the specific training required to address it.

Table:

Risky Behavior	Root Cause	Training Need
Ex: Clicking phishing links	Ex: Don't check sender/URLs	Ex: Train on spotting phishing and reporting emails

---

Phase 3: Choosing Effective Delivery Methods

Next, for each training need you identified, select the most suitable delivery format. Consider options like micro-modules, phishing simulations, posters, workshops, newsletters, or a "tip-of-the-week".

Justify why the chosen format is the most effective way to address the specific risk.

Here are some examples:

- **Phishing:** Use a combination of a monthly phishing simulation and a short, two-minute refresher video.

- **Weak Passwords:** Implement a 15-minute training module and include a reminder during employee onboarding.

Phase 4: Defining Success Metrics

Decide how you will measure the success of each training effort. Your metrics should focus on **behavioral change**, not just on completion rates.

Examples of behavior-focused metrics include:

- Reducing the phishing click rate from 15% to 5% within six months.
- Increasing the number of reported suspicious emails by 30% in three months.
- Achieving 95% multi-factor authentication (MFA) enrollment within 90 days.

Phase 5: Finalizing the Plan

Consolidate all decisions into a single, one-page **Security Awareness Plan**. The plan should include the following sections:

- Purpose
- Behavior Risks
- Target Audience
- Training Needs
- Delivery Formats
- Success Metrics

Final step, implementing the new security plan.