

PhishLabs Training and Education Model

Why a Short, Focused, and Frequent security awareness training model reduces organizational risk

Despite decades of research about how adults learn, many organizations continue to follow an antiquated model of training design that is counterproductive to their goals. When it comes to security awareness, reducing risk to the company and your employees is paramount. There is little room for error and inefficiencies, so when an organization invests in security education it must be effective.

At PhishLabs we employ the Short, Focused, and Frequent (SFF) model that is designed for how adults learn. The model complements a foundation of learning with regular, highly-focused microlearning modules.

These one-to-five minute engaging modules delivered monthly that reinforce a single learning objective. For example, a learner would see a single two-minute module on password security instead of a one-hour video on general awareness tips with dozens of key points. Combined, these learning activities create a powerful education model designed for adult learners to retain and use the information they receive.

The Problem

Research shows that **learners forget up to 60 percent of content presented in a traditional training environment in a single day**. Lengthy courses disregard cognitive load, memory, and attention; providing so much information that learners fail to process much of anything. Many programs also take a one and done approach, never reinforcing learning objectives and further contributing to a lack of retention.

Organizations cannot afford for their employees to forget 60 percent of good security behaviors.

Our Solution

This particular education model tackles this problem by balancing the capabilities of technology with those of the human mind. Highly interactive micro-modules make the most of learner attention and never present more information than one can process or ultimately remember.

Interactions are designed with a high degree of fidelity, often emulating the task itself to facilitate behavioral transfer on the job. The more realistic the simulated environment, the more likely your employees will practice what they have learned.

The model is designed to improve the organizational outcomes from your training investment. As a result of more effective training you will see reporting of suspicious emails increase, clicks on targeted attacks decline, and company security increase overall.

Engaging, White Labeled Solutions

In addition to engaging learning experiences, PhishLabs understands the importance of each organization's unique policies, procedures, and culture. All training programs can be tailored with your requirements and culture in mind, even including white labeling options.