SOPHOS
Security made simple.

Designing a Phishing Simulation and Security Awareness Training Program

Getting the most out of Sophos Phish Threat requires a little bit of upfront thought and planning. If it's your first time designing a phishing assessment and training program, you may feel unsure of where to start. This document offers some best practices and a sample program outline to get you started.

Start with on-boarding

Before jumping right in, we recommend taking some initial steps to set the foundation for an effective program.

Get a baseline

Measuring change in behavior is key to demonstrating the value of your program. Start by running a baseline assessment with all users. We recommend choosing a template with **Moderate** difficulty to help you determine where you stand.

Announce your program

Getting users to "buy in" is critical to effective training. Send an email to all users to explain what you're doing and why. Share the results of your baseline test and identify what users should have looked out for. Avoid giving the impression that users are being punished or that you are out to trick people.

Set up for success with training

Finally, set users up to succeed by enrolling everyone in an initial **Training Campaign.** Choose a training module that reinforces the basics of phishing attacks or social engineering. We recommend our **Basic Phishing** or **Ten Ways to Spot a Phish** training.

Have a plan

The most common mistake we see organizations make is launching their first assessment without a plan. With a little upfront effort, you'll put yourself in position to affect positive change and show real results. Let's dig in to the key concepts of our sample program.

Who to target

We'll assume you want to improve the security awareness of your whole organization. If you're focusing on only a subset of your users, you can still apply this advice to the smaller group.

Our program tests every user quarterly by enrolling one-third of our organization in a campaign each month. By breaking your campaigns up this way, you introduce more variability to your program's schedule, making sure that users stay on their toes.

Degree of difficulty

We recommend most organizations start with an **Easy** assessment the first quarter. But, if your baseline measurement was strong (10% or less), you may want to start with a **Moderate** or even **Hard** attack template. The key is to adapt to the needs of your organization. In subsequent quarters, tune your difficulty up or down based on the last quarter's results.

Vary attack styles

You'll be surprised what people fall for (and what they don't!). Make sure you introduce a variety of attack types and styles to your users. We recommend using at least one of each type of attack each year: **Phishing**, **Credential Harvesting**, and **Attachments**.

Analyze and share results

At the end of each quarter, take some time to run reports and make sense of your results. What's going well? Where is there room for improvement? Don't keep your findings to yourself. After all, it's your users who will benefit the most from these insights. Sharing with them will reinforce what they've learned and promote the right behavior.

Sample 12-Month Program

Our sample program outline illustrates the basic structure of a simple, iterative, annual program. The key is to adjust the program to your needs. Think about your goals and the particular needs of your organization and tailor your program to fit.

Phase	Action	Target Users
Onboarding	Baseline assessment	All users
Onboarding	Intro email	All users
Onboarding	Training campaign	All users

Start of Quarter 1	Divide users in 3 equal-sized groups (A, B, C)	
Month 1	Phishing campaign (Easy)	Group A
Month 2	Phishing campaign (Easy)	Group B
Month 3	Phishing campaign (Easy)	Group C
End of Quarter 1	Analyze and share results	
Start of Quarter 2	Divide users in 3 equal-sized groups (D, E, F)	
Month 4	Credential Harvesting campaign (Moderate)	Group D
Month 5	Credential Harvesting campaign (Moderate)	Group E
Month 6	Credential Harvesting campaign (Moderate)	Group F
End of Quarter 2	Analyze and share results	
Start of Quarter 3	Divide users in 3 equal-sized groups (G, H, I)	
Month 7	Phishing campaign (Hard)	Group G
Month 8	Phishing campaign (Hard)	Group H
Month 9	Phishing campaign (Hard)	Group I
End of Quarter 3	Analyze and share results	
Start of Quarter 4	Divide users in 3 equal-sized groups (J, K, L)	
Month 10	Attachment campaign (Moderate)	Group J
Month 11	Attachment campaign (Moderate)	Group K
Month 12	Attachment campaign (Moderate)	Group L
End of Quarter 4	Analyze and share results	

Tips to remember

Keep these best practices in mind when designing your program.

Don't be predictable

Avoid easily detectable patterns such as launching your campaigns on the first of each month or using the same template in consecutive quarters. Keeping your users guessing will ensure realistic assessments.

Think seasonally

Attackers will often piggyback on seasonal trends. February, March, and April are a great time for a tax-themed simulation. Likewise, November and December are great for ecommerce-themed attacks. Think about the timing of your simulations to maximize effectiveness.

Avoid shaming

While it's important to follow up with users who fall for a simulation – particularly if they are chronic offenders – we recommend using positive reinforcement, not punishment. Releasing the names of users is rarely a good idea. Instead, send follow-up materials to those who fail or consider enrolling them in additional training.

Step up your game

Once you've mastered the basics, it's time to incorporate some more advanced techniques into your program.

Auto-enroll new users

Many organizations see new users as their biggest area of risk. They're unfamiliar with your policies and haven't been tested and trained. Using the **Auto-Enroll New Users** feature, Sophos Phish Threat enables you to set up an ongoing campaign to which all new users will be added.

Spend extra time on the repeat offenders

Seeing the same names over and over again in your reports? It's time to provide some individualized attention. In some cases, we recommend testing repeat offenders monthly until behavior improves.

Focus on high-risk users

Our basic program ignores the particular threats users in certain roles face. Your Finance and Accounts Payable departments are frequent targets of real attackers, as are senior executives. Consider separating these users from the general population and testing them with simulations designed to target their specific functions in your organization.

Introduce rewards

To really ramp up engagement among your users, come up with a rewards program that recognizes the top performing users and departments. Simple things like publishing a company-wide leaderboard or offering a free lunch are easy, cost-effective ways to get people motivated.