ISECOM

INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

SALT

Security Awareness Learning Tactics

Client:	Public
Date:	
Class:	Open
Version:	v3 DRAFT
Author:	Pete Herzog

Open Source Security Testing Methodology Manual

OSSTMM

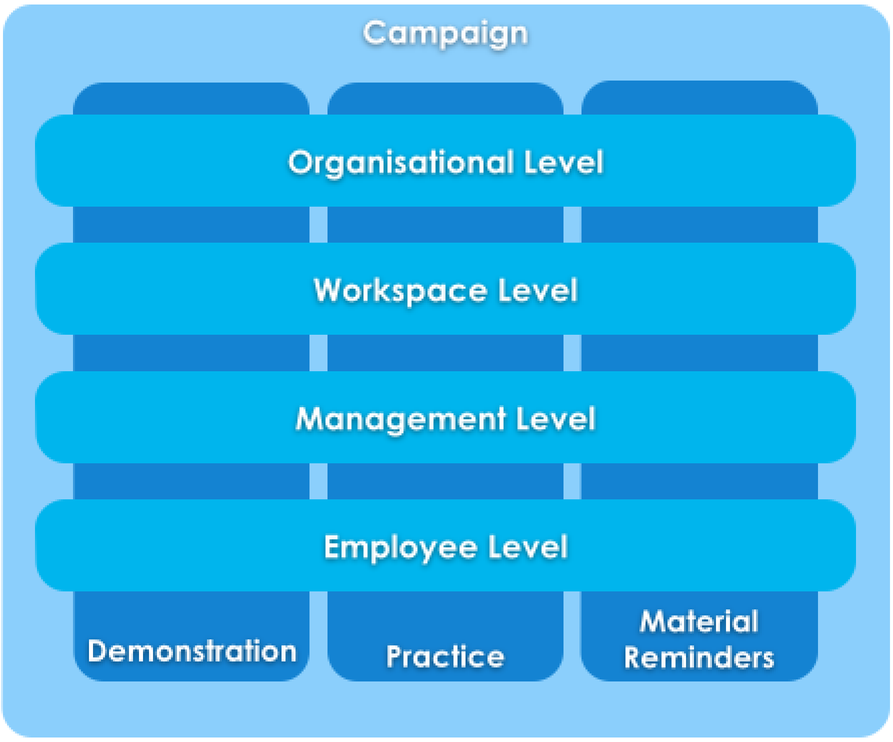
www.osstmm.org

This document provides details on creating Security Awareness programs.

Quick Page Guide:

Using this Guide

This manual uses a guideline to create and manage an improved security culture and change behaviors in people to be more security minded. This guide points out optimal changes, however it does not express precisely how to make these changes. In some cases, specific examples may be used for clarity, however examples should not be seen as required methods or narratives to be used. This leaves the execution of these guidelines flexible to the requirements and regulations of the user.



Campaign

1. Prepare a budget for materials and training. Dedicate a person, like an internal "blogger," for maintaining interesting news and videos to share with employees extensions of what they learn in the Demonstration and during Practice.

2. Assure management-level support through the organization. Include them in all training, as well.

3. Make quantitative measurements based on incidents and support requests during months of applied security awareness.

4. Make regular qualitative assessments through inverse questionnaires: asking how employees think their peers are performing/standing in the program to reduce bias caused by false reflection.

5. Have an empty, stylish, clean, and plain classroom available to regularly train groups in short sessions and scented with citrus.

6. Create a short and direct security policy of specific tasks rather than "do and don't" rules to be read and signed. For example, a direct task may be to require all incoming calls from existing vendors be returned rather than accepted directly. Even if following compliance directives, re-write those directives into tasks that can be clearly understood.

7. Prepare material reminders and practice sessions ahead to be delivered regularly at the start of the program. Consistency builds rapport, trust and habit.

8. Have a readily available security help and support number to answer questions and a staff employee who can investigate potential problems. This support service operates anonymously for those who get help. The support line keeps statistics for metrics and strategy decisions, however it only serves to reward employees for using it and helping find problems. This is necessary to help employees adapt to a more secure behavior.

Material Reminders

9. Avoid paraphernalia of paranoia. Keep reminders happy, friendly, and positive. Avoid materials with mistrust, dour faces, watching eyes and fear.

10. Use material reminders to have employees practice security skills, promote happier working conditions, reduce anxiety, exercise and encourage quiet breaks.