Julio Pochet – Choosing the Right Tools for MeCo's SETA Program

To help MeCo build a strong Security Education Training and Awareness (SETA) program, I researched two reliable sources: **NIST** and **SANS Institute**. Both offer valuable tools and guidance for setting up a program that actually works.

NIST SP 800-50 Rev. 1

NIST SP 800-50 Rev. 1 (from www.nist.gov) is a government-published guide that focuses on creating a Cybersecurity and Privacy Learning Program. It breaks the process down into four steps: assess training needs, design learning content based on job roles, implement the program, and evaluate how it's doing. This approach is great for building something long-term and aligns well with compliance and risk management goals.

Assess Training Needs

Identify security knowledge gaps and requirements

Design Learning Content

Create role-based security training materials

Implement Program

Roll out the training across the organization

Evaluate Effectiveness

Measure results and make improvements

SANS Security Awareness Toolkit

The **SANS Security Awareness Toolkit** (found at www.sans.org) takes a more practical and ready-to-use approach. It includes templates, posters, training videos, and campaign materials to help you quickly launch security awareness efforts.

One of the best examples is their "Working Securely from Home" guide, which focuses on real-world risks like phishing, weak passwords, and unpatched systems. It's designed to be engaging and easy to understand, even for non-technical users.

Ready-to-Use Materials

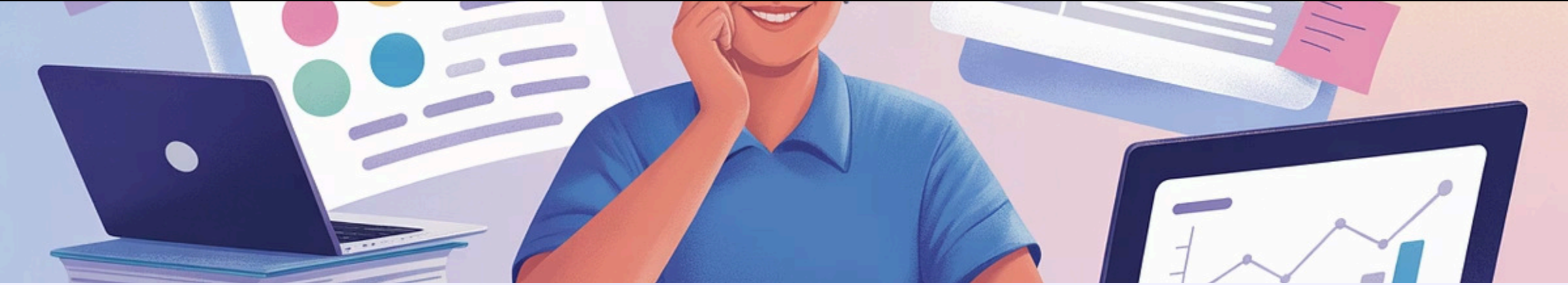
Templates, posters, videos, and campaign resources

Practical Focus

Real-world security risks and solutions

User-Friendly

Engaging content for non-technical employees



My Pick

Foundation: NIST SP 800-50

I recommend using **NIST SP 800-50** as the foundation because of its structure and flexibility.

Enhancement: SANS Materials

But combining it with **SANS materials** would make the rollout more engaging and user-friendly—especially for employees who aren't cybersecurity experts.