

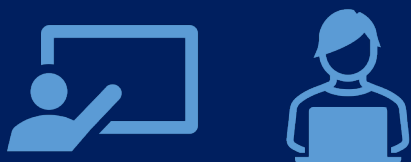
Evaluating Skills-Based Training for Employee Risk Recognition and Reporting of Malicious Elicitations

Government and critical infrastructure industry organizations are constantly trying to help their employees more easily identify and report security risks. Traditionally, only awareness or information-based training has been used to educate the workforce about security risks which can have limited effectiveness. It is unclear whether other forms of training like skills-based training—where people practice what they learn—can bolster security risk recognition and reporting.

What are Awareness-Based and Skills-Based Training?

Awareness-Based Training (current model)

Employees *recognize* and *report* risk through passive, information-based training



- Rarely evaluated for effectiveness
- Poor information retention by employees
- Employees fail to apply training to real world

Example: Learning how to ride a bike by watching a video about riding a bike.

Skills-Based Training

Extend awareness-based training with *practice* and *feedback*



- Skill acquisition is a process
- Active information synthesis (through doing)
- Feedback (how are you doing)

Example: Learning how to ride a bike by riding a bike, including falling off.

Applied Research Study



In 2023, MITRE's behavioral scientists and insider risk subject matter experts conducted a 12-month behavioral experiment to assess the effectiveness of skills-based security training over traditional annual security training to increase recognition and reporting of malicious e-mail elicitation.

Malicious elicitation are techniques strategically used in conversation (i.e., in writing, over the phone, in person, or online) with the sole purpose of collecting sensitive, non-publicly available information about business operations or technological assets without raising suspicion. To an untrained observer, a skilled elicitor can make conversations seem analogous to professional networking situations experienced over e-mail or at conferences. The similarity causes challenges as employees are encouraged to safely navigate professional activities (e.g., networking), whilst remaining vigilant to malicious elicitation.

Evaluating Skills-Based Training for Employee Risk Recognition and Reporting of Malicious Elicitations

Behavioral Experiment Methodology

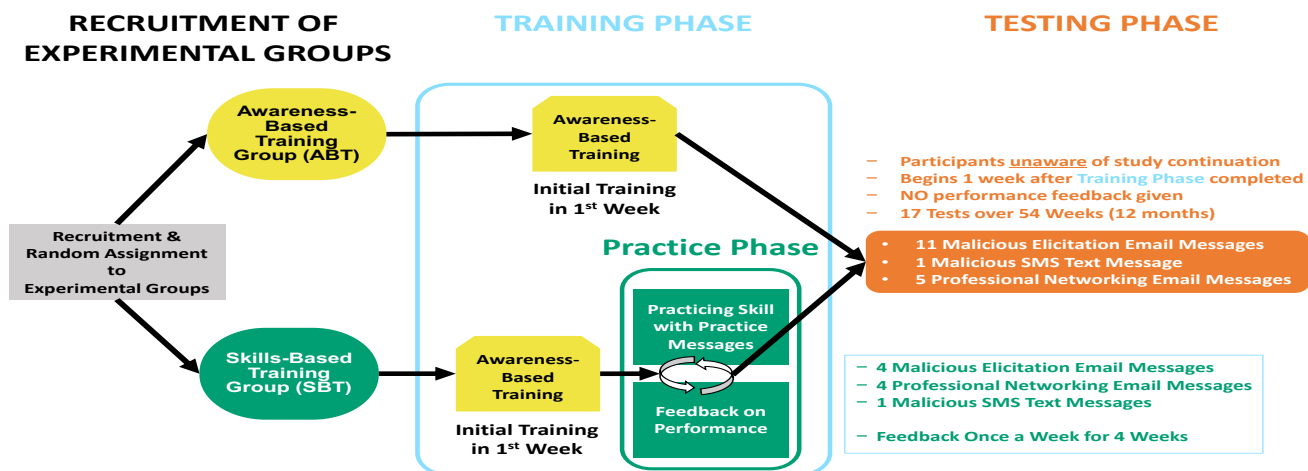
72 real employees of a U.S. defense industrial base organization were randomly assigned to either:

-  Traditional annual Awareness-Based Training (ABT) group, or
-  Skills-Based Training (SBT) group that included practice and feedback.

Both employee groups received the same initial awareness-based training on malicious elicitations, which was a standard 30-minute computer-based training. The SBT group also received a skills-based training with practice and feedback with real professional networking and malicious elicitation messages sent periodically over 5 weeks.

After receiving training, both the ABT and SBT employee groups were periodically sent professional networking and malicious elicitation messages for 54 weeks – via e-mail and text messaging. The researchers were integrated with the organization's reporting channels, and able to determine whether employees reported specific messages or not.

Figure 1: Behavioral Experiment Methodology Phases



Findings

Employees in the Skills-Based Training (SBT) group consistently reported more malicious e-mail elicitation messages than employees in the Awareness-Based Training (ABT) group. To a much lesser extent, the SBT group reported benign, professional networking e-mail messages more often than the ABT group. Patterns were consistent across characteristics such as gender and high risk roles.

Conclusions

With only 5 weeks of practice—consisting of only minimal time effort to read 9 e-mails and report 4 of them—employees who had skills-based training showed a 25% improvement over traditional training and the new skill to identify malicious e-mail elicitation messages lasted for up to 12 months.

*For a more detailed brief, please contact:
Dr. Deanna D. Caputo, Chief Scientist for Insider Threat Research & Solutions
E-Mail: dcaputo@mitre.org*



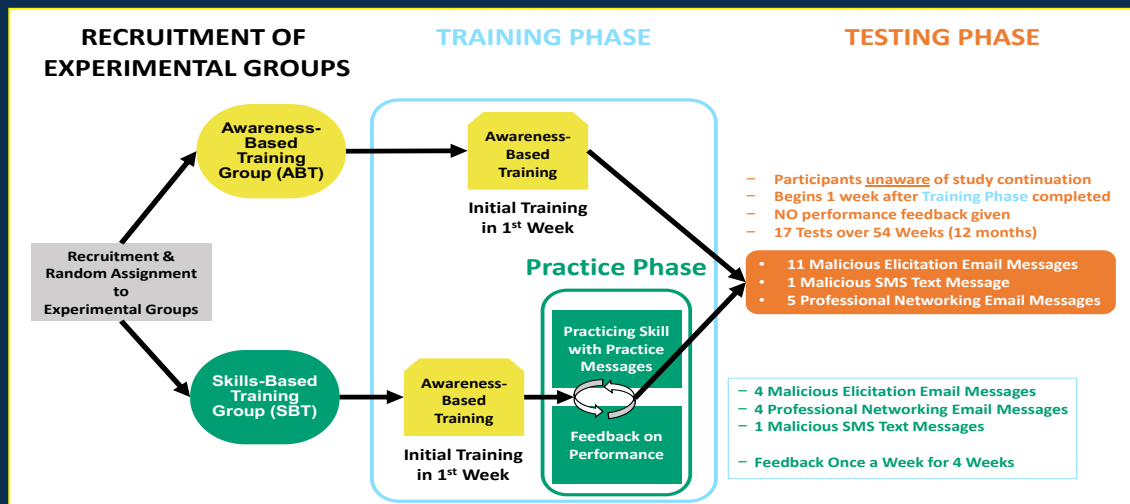


“EMPLOYEES WHO RECEIVED SKILLS-BASED TRAINING SHOWED SIGNIFICANT INCREASED REPORTING OF MALICIOUS ELICITATIONS FOR UP TO 12 MONTHS”

Improving Risk Recognition and Reporting with Skills-Based Training

BACKGROUND & DESIGN

- Experimental study of 72 real employees over 12-months examined the effectiveness of skills-based security training over traditional annual security training to increase awareness and reporting of malicious elicitations.
- Employees randomly assigned to a traditional annual *Awareness-Based Training (ABT)* group or a *Skills-Based Training (SBT)* group that included practice and feedback.



FINDINGS

Employees in the SBT group consistently reported more malicious e-mail elicitations than those in the ABT group. To a much lesser extent, SBT participants reported benign, professional networking e-mail messages more often than the ABT group. Patterns were consistent across characteristics such as gender and high risk roles.

CONCLUSIONS

With only 5 weeks of practice—consisting of a minimal time effort to read 9 e-mails and report 4 of them—employees who had skills-based training showed a 25% improvement over traditional training and the new skill to identify malicious e-mail elicitations lasted for up to 12 months!