General Description

The measurement system for the ACES phishing module aims to gather clear, simple, and direct feedback from session participants, at two points: before and after the session. Its purpose is to evaluate the effectiveness of the training session without requiring any prior technical knowledge or subjecting participants to complex procedures. The questionnaire is designed to be accessible and user-friendly, ensuring that all responses accurately reflect participants' learning and perceptions in an uncomplicated and efficient manner.

The proposed tools are two short, self-administered surveys: a pre-assessment completed at the beginning of the session to understand participants' profiles and measure their initial knowledge, and a post-assessment completed at the end of the session to evaluate learning improvement and gather feedback. Together, they allow us to:

- Understand the general profile of participants (age, country, gender).
- Identify changes in which key concepts were understood (e.g., phishing signs, safe responses).
- Gather participants' views on the clarity, usefulness, and relevance of the content.
- Measure their interest in continuing to learn about digital safety.

More than an administrative process, this measurement is meant to be a tool for continuous improvement. It helps adjust content, understand what works, and strengthen future sessions. It also provides concrete evidence that supports the broader goal of bringing digital safety education to local communities, empowering end users to face the growing risks of online fraud.

Metrics derived from survey

Question	Metric	How it is interpreted
Pre-assessment – Country	Countries reached	Geographic distribution per session
Pre-assessment – Age	Age group distribution	Identify the most engaged age ranges
Pre-assessment – Gender	Gender distribution	Measure basic inclusion and diversity
Pre and post – Question on phishing signs	% of correct answers before and after	Percentage change indicating improvement in recognizing phishing signs
Pre and post – Question on correct action	% of correct answers before and after	Percentage change indicating improvement in response to suspicious emails
Post-assessment – Most useful topics selected	Topics with the highest number of mentions	Qualitative insight to adjust or reinforce content
Post-assessment – Content clarity	% rating content as "clear"	Pedagogical effectiveness indicator
Post-assessment – Session recommendation	% who would recommend the session	Overall satisfaction metric
Post-assessment – Interest in future sessions	% interested in future sessions	Follow-up engagement potential

Post Assessment / Survey

Estimated Duration: 5 minutes
When to Apply: At the end of the session

Learning measurement

Knowledge Check

1. **Select two common warning signs in a phishing email (Select all that apply)**
   ☐ It uses alarming or urgent language
   ☐ It promises prizes or unbelievable offers
   ☐ It comes from a strange or misspelled address
   ☐ I'm not sure
2. **What should you do if you receive a suspicious email? (Select only one)**
   ☐ Share it with friends or contacts
   ☐ Report it and avoid clicking
   ☐ Open the attachment to check it
   ☐ I don't know
3. **Which of the following topics did you find most useful in the session?**
   ☐ How to identify fake emails
   ☐ Digital security tips
   ☐ How to explain phishing to others
   ☐ Other: _____

Session Feedback

7. **Was the information clear and easy to understand?**
   ☐ Yes ☐ Somewhat ☐ No
8. **Would you recommend this session to others?**
   ☐ Yes ☐ No
9. **Would you like to attend more sessions like this?**
   ☐ Yes ☐ No