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

Pre-Assessment / Survey

Estimated Duration: 3-5 minutes
When to Apply: At the start of the session

Pre-knowledge measurement

1. What is phishing?

   ☐ A program used to make computers faster
   ☐ **A type of online fraud used to steal personal information**
   ☐ A video calling application
   ☐ A file backup system

2. Pick two common signs of a phishing scam.

   ☐ The email uses typo-filled or strange sender addresses
   ☐ The content uses alarming or urgent language
   ☐ It offers unbelievable rewards or suspicious prizes
   ☐ Not sure
   ☐ **All of the above**

3. Why do cybercriminals use messages that create urgency or fear?

   ☐ To improve the design of the message
   ☐ **To make people act without thinking**
   ☐ To reduce the file size
   ☐ To comply with security regulations

4. What is the best action to take if you suspect that a message may be phishing?

   ☐ Ignore it and open it later
   ☐ Forward it to all your contacts
   ☐ **Report it and do not share personal information**
   ☐ Reply to confirm if it is rea

5. What should you check first when receiving an unexpected email from a bank or institution?

   ☐ **The sender's email address**
   ☐ The font style used
   ☐ The color of the logo
   ☐ The length of the message

Post Assessment / Survey

Estimated Duration: 5 -7 minutes
When to Apply: At the end of the session

Learning measurement

Knowledge Check

1. Which of the following is the most effective way to identify a phishing email?

   ☐ Checking if the message includes colorful images
   ☐ **Verifying the sender's email address and looking for suspicious language**
   ☐ Opening the attachment to see what it contains
   ☐ Replying to ask if the message is legitimate

2. Why should you avoid clicking on links from unexpected emails or messages?

   ☐ **Because they may contain malware or lead to fake websites designed to steal information**
   ☐ Because they make your computer run slower
   ☐ Because they automatically delete your files
   ☐ Because they use too much internet data

3. What is the safest response when a message asks for your password, banking details, or personal information?

   ☐ Provide the information if the message looks professional
   ☐ Ignore security warnings and respond quickly
   ☐ **Verify the request through an official source before taking action**
   ☐ Send only part of the information requested

4. How does enabling two-factor authentication (2FA) improve cybersecurity?

   ☐ It makes internet speed faster
   ☐ **It adds an extra layer of security beyond just a password**
   ☐ It automatically blocks all spam emails
   ☐ It removes the need for passwords

5. If you accidentally click on a suspicious link, what should you do first?

   ☐ Continue browsing normally
   ☐ **Immediately report it and change passwords if necessary**
   ☐ Ignore it if nothing happens
   ☐ Forward the link to a friend for advice

6. Why is cybersecurity awareness important for everyone, not just IT professionals?

☐ **Because cyber threats can affect anyone who uses digital devices and the internet**
☐ Because only businesses are targeted by cybercriminals
☐ Because cybersecurity is only needed for online shopping
☐ Because antivirus software solves all security problems

Session Feedback

7. 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: _____

8. Was the information clear and easy to understand?
☐ Yes ☐ Somewhat ☐ No

9. Would you recommend this session to others?
☐ Yes ☐ No

10. Would you like to attend more sessions like this?
☐ Yes ☐ No