Co-funded by the European Union

BY NC SA

This project has been co-financed with support from the European Commission's ERASMUS+ programme. This publication reflects only the views of its authors, and neither the European Commission nor SEPIE can be held responsible for any use that may be made of the information contained herein.

LEARNING BOX OF UNPLUGGED ACTIVITIES

"Is This Safe?" – Understanding Digital Risks

In this activity, participants examine everyday digital situations involving suspicious messages, emails, and phone calls. Working collaboratively, they assess the level of risk, identify warning signs, and decide on the safest course of action. They also learn how to protect their personal and financial information and verify requests before responding. By the end of the activity, participants will have developed simple, practical, and repeatable rules for using digital services more safely and confidently.

Target Group

☑ Low-skilled adults with low digital competences
☑ Low-skilled adults with limited formal education or qualifications
☑ Low-skilled adults with low participation in lifelong learning / training opportunities

Learning Objectives

- Break down a digital communication or request into clear and manageable steps.
- Recognise common warning signs of suspicious or unsafe digital communication.
- Identify sensitive information that must be protected, such as passwords, banking details, and personal data.
- Apply simple decision-making rules to determine the probably safest response.
- Explain and demonstrate safe decisions clearly during role-play activities.

Theme

Information Literacy Competences

Duration

90-120 minutes

Level

Advanced

Computational Thinking Steps Used

☑ Decomposition
☑ Pattern recognition
☑ Abstraction
☑ Algorithmic thinking

Competence Areas

a) Innovation Competences

☑ Creativity
☑ Critical thinking
☑ Problem solving
☑ Communication
☑ Collaboration

Methodological Approach

- ☑ Gamification
- ☑ Challenge-Based Learning
- ☑ Collaborative learning
- ☐ Experiential learning

b) Information Literacy Competences

- ☑ Ability to access, understand, and critically analyse information
- ☑ Interpretation of digital and visual content
- ☑ Awareness of media influence and biases

c) Life and Career Competences

- ☑ Flexibility and adaptability
- ☑ Initiative and autonomy
- ☑ Sociability and intercultural competence
- ☑ Productivity
- ☑ Leadership and responsibility

Learning Outcomes

By the end of the activity, participants will be able to:

- Break down a digital situation into clear and manageable steps;
- Identify common warning signs in suspicious or unsafe messages, emails, and phone calls;
- Distinguish between probably safe, potentially risky, and unsafe actions;
- Apply simple safety algorithms to protect personal, financial, and login information;
- Choose and explain an appropriate response to everyday digital risks;
- Demonstrate probably safer decision-making during role-play situations.

Notes

- Use simple and realistic examples, such as text messages, emails, phone calls, and online requests.
- Select situations that are familiar and relevant to participants' everyday lives.
- Encourage discussion and the voluntary sharing of experiences without pressuring participants to disclose personal information.
- Provide guidance when necessary while allowing participants to analyse situations and make their own decisions.
- Use clear, accessible language and explain any unfamiliar digital terms.
- Emphasise that anyone can be deceived by a convincing message and that asking for help is a

sensible safety strategy.

- Reinforce the importance of stopping, checking, and verifying a request before responding, clicking a link, or sharing information.

Step 1. Decomposition

Adult learners receive printed cards describing simple and realistic digital scenarios, for example: "You receive a message asking for your bank details" (Appendix 1), "You receive a phone call asking you to provide your password" (Appendix 2).

Adult learners are asked to:

- Break each situation down into smaller and more manageable steps;
- Identify who initiated the communication and how contact was made;
- Determine what information or action is being requested;
- Identify what the recipient is expected to do;
- Consider the possible consequences of following the request.

Facilitator support:

- Facilitator may ask: "What happened first?", "What does the person want?", "What might happen if the recipient follows the request?"
- Help adult learners focus on one aspect at a time;
- Emphasize understanding the situation clearly.

This step helps adult learners understand digital situations in a simple and structured way.

Step 2: Pattern Recognition

Adult learners receive additional examples of digital messages, emails, phone calls, and online requests.

They are asked to compare the different situations and identify similarities and differences.

Recognise recurring warning signs, such as:

- Requests for personal, financial, or login information;
- Urgent or threatening language, such as "act now!";
- Unknown or unexpected senders;
- Suspicious links or attachments;
- Offers, prizes, or promises that appear unrealistic;

- Pressure to respond without checking the information.

Facilitator support:

- Facilitator may ask: “What looks suspicious?”, “Have you seen something like this before?”
- Highlight repeated warning signs;
- Encourage sharing personal experiences.

This step helps adult learners recognise recurring patterns in suspicious digital communication and apply this knowledge when assessing unfamiliar situations.

Step 3: Abstraction

Adult learners focus on the essential elements needed to assess whether a digital situation is probably safe, suspicious, or unsafe.

They are asked to:

- Identify sensitive information that must be protected, such as passwords, banking details, verification codes, and personal data;
- Distinguish relevant warning signs from less important details;
- Identify the main risk presented by each situation;
- Decide whether the communication is likely to be probably safe, requires further verification, or is unsafe;
- Formulate simple safety principles that can be applied in similar situations.

Facilitator support:

- Facilitator may ask: “What information should never be shared?”, “Which detail is most important for assessing the risk?”, “What can be ignored because it does not affect the decision?”
- Emphasize simple safety rules.
- Help adult learners focus on key risks.

This step helps adult learners simplify complex digital situations, focus on the information that matters most, and make more informed safety decisions.

Step 4: Algorithmic Thinking

Adult learners develop (individually or in groups) a clear, step-by-step algorithm for responding safely to suspicious digital communication. The algorithm should guide a user from the moment a message, email, or phone call is received to the final decision and appropriate action.

Adult learners are asked to:

- Define the main steps of the decision-making process;
- Arrange the steps in a logical sequence;
- Include decision points using if–then rules;
- Specify what action should be taken in each situation;
- Visualise the algorithm using cards, arrows, symbols, or a simple flowchart.

The algorithm may include the following sequence:

- Receive the communication.
- Identify the sender and the communication channel.
- Determine what information or action is being requested.
- Check for warning signs, such as urgency, threats, suspicious links, unexpected requests, or requests for sensitive information.
- Decide whether the sender can be verified.
- Choose the appropriate response.

Example decision rules:

- If the sender is unknown, then do not respond immediately.
- If the communication requests a password, verification code, or banking information, then do not share it.

Finally, adult learners:

- Test their safety assurance algorithms through role-play situations;
- Explain and justify their decisions;
- Compare the different algorithms developed by the groups;
- Identify which rules are most useful in real-life situations;
- Revise their decision-making process when necessary.

Facilitator support:

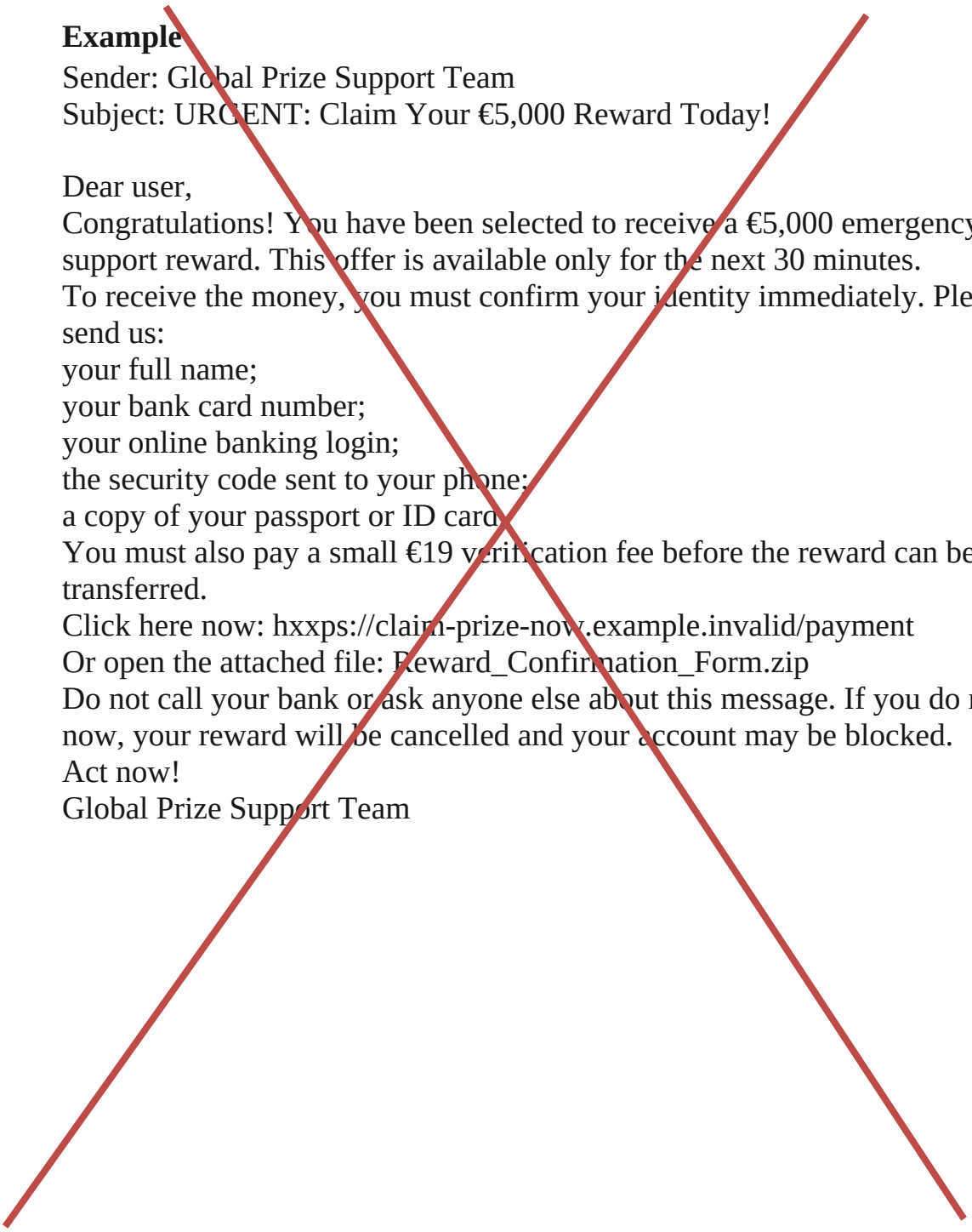
- Facilitator may ask: “What should the user do first?”, “What decision must be made at this point?”
- Encourage critical thinking for decision-making.
- Reinforce safety assurance habits.

This step helps adult learners transform general safety principles into a clear, structured, and repeatable decision-making algorithm.

Example

Sender: Global Prize Support Team
Subject: URGENT: Claim Your €5,000 Reward Today!

Dear user,
Congratulations! You have been selected to receive a €5,000 emergency support reward. This offer is available only for the next 30 minutes.
To receive the money, you must confirm your identity immediately. Please send us:
your full name;
your bank card number;
your online banking login;
the security code sent to your phone;
a copy of your passport or ID card.
You must also pay a small €19 verification fee before the reward can be transferred.
Click here now: hxxps://claim-prize-now.example.invalid/payment
Or open the attached file: Reward_Confirmation_Form.zip
Do not call your bank or ask anyone else about this message. If you do not act now, your reward will be cancelled and your account may be blocked.
Act now!
Global Prize Support Team



Appendix 2

Caller: Good afternoon. I am calling from your bank's security team. Someone is trying to withdraw €1,000 from your account. We have only five minutes to stop the transaction.

You: What do I need to do?

Caller: Give me your online banking password immediately so I can secure your account.

You: Why do you need my password?

Caller: This is an emergency. If we delay, you could lose your money. You must also transfer €500 to a temporary "safe account". We will return it once your account is secure.

You: I would like to call my bank first.

Caller: There is no time! Stay on the line and follow my instructions now. Tell me your password.

