Co-funded by
the European Union

STORIES
4 WINGS

PRACTICAL ACTIVITY AND GAME

Stories4Wings

2024-1-ES01-KA220-ADU-000255317

Technology Literacy

Freedom Under Password

AIFED

l.i.n.c.

avanzo

SWIPEA

Freedom Under Password

Technology Literacy

This document includes a **practical activity and a game** to further explore and reflect on the value, skill, or competency of each story.

This activity and game serve as a **supplementary learning tool** to the guide with the questions and reflections, approaching learning from a **playful, active, and participatory perspective**.

These activities aim to reinforce learning through **practice and direct experience.**

Freedom Under Password

Technology Literacy

PRACTICAL ACTIVITY

1

Educational Objectives

- Identify basic password requirements
- Create memorable and secure passwords
- Evaluate password examples and explain why they are good or bad
- Understand the risks of reusing or sharing passwords.

Number of Participants

6–12

Duration

45-60 minutes

Materials Needed

- Blank index cards
- Markers
- Printed sheet with password rules
- Printed participant card with 8 password examples
- Flipchart or whiteboard

Freedom Under Password

Technology Literacy

Activity Description

1.Opening. Read the story extract about Sven creating a password.

“I had to create a password: eight digits, one capital letter, and a special symbol. ... They advised me to use different passwords for every app, but for today... I’ve had enough digital immersion.”

2.Guided discussion. Ask the participants:

What made Sven confused? What is a “special symbol”? Note answers on the board.

3.Demonstration. Show Card Set A (password requirements and examples). Explain each requirement in plain language and with one pictogram:

A1. Requirement: 8 characters — Example: House2024

A2. Requirement: 1 uppercase letter — Example: SunSea!7

A3. Requirement: 1 symbol — Example: bread@1234

A4. Do not reuse — Tip: One password per service

Freedom Under Password

Technology Literacy

A5. Mnemonic phrase — Example: MyDogEats!8

A6. Avoid obvious data — Tip: No family names or birthdates

A7. Secure combination — Example: Red!Street9

A8. Remember without writing — Tip: Use a short rehearsable phrase

4. Integrated extra exercise — evaluate examples:

Give each participant the printed list of 8 password examples (below).

Individually they mark Good/Bad and write one short reason.

Good or bad?

- Sunset!2024
- -P@ssw0rd
- Anna1978
- BlueCar
- MyDogEats!8
- qwerty123
- Red!Street9
- !TrainHouseLong

Freedom Under Password

Technology Literacy

Key:

- Sunset!2024 - Good - Long phrase + symbol + numbers; memorable and hard to guess.
- P@ssw0rd - Bad - Common pattern (password → leetspeak); widely known and weak.
- Anna1978 - Bad- Personal name + birth year; easy to guess from public info.
- BlueCar - Bad - Short dictionary words only; lacks symbol/number/mixed case.
- MyDogEats!8 - Good - Phrase-based, includes symbol and number; unique and memorable.
- qwerty123 - Bad - Keyboard pattern + simple numbers; extremely common and insecure.
- Red!Street9 - Good - Mixed elements (word + symbol + number + uppercase) and length.
- !TrainHouseLong - Good - Long phrase with symbol and mixed case; high entropy and
- memorable.

Freedom Under Password

Technology Literacy

5. Check in pairs and then in group.

6. Paired exercise — create passwords: In pairs, give each pair three requirement cards from Card Set A. Pairs create three example passwords that meet the requirements and write a short mnemonic phrase for each. Emphasize fictional examples only.

7. Group review and feedback: Go through their examples aloud, ask the students to state their choice and reason for each, then reveal the facilitator answer key and give some explanation.

8. Wrap up: Reinforce three simple rules: (1) use long, unique phrases; (2) include symbol/number/mixed case; (3) never share or reuse passwords.

Freedom Under Password

Technology Literacy

2

GAME

Educational Objectives

Truth or Myth — Digital Safety

- Help participants distinguish common myths from facts about passwords
- Privacy and basic digital safety
- Practice quick decisions and short explanations.

Number of Participants

6 - 15

Duration

20-25 minutes

Materials Needed

- Two large posters labeled TRUTH and MYTH
- Printed statement cards (see below)
- Optional pictograms

Freedom Under Password

Technology Literacy

Activity Description

1. Introduction

Explain the game: you will read a statement and the students have to move towards TRUTH or MYTH posters.

2. Rounds:

The facilitator reads one card aloud. Participants move to the poster they think is correct. Give participants 10–15 seconds to move to a side. Ask one volunteer from each side to give a one-sentence reason. Reveal the correct answer using the key and add one short practical tip if you want.

Statement cards (print each line on a separate card):

- If you forget the password, the app recovers it automatically.
- Using the same password everywhere increases risk.
- Short passwords are just as secure as long ones.
- Asking an official office for help is safer than sharing passwords.

Freedom Under Password

Technology Literacy

- Sharing a password with a friend is fine if you trust them.
- Do not share passwords; ask for help without giving them.
- Any symbol makes a password secure.
- A long, unique phrase is often easier to remember and more secure.
- If someone has your phone number, they can access all your apps.
- Some apps ask for a photo of your ID; always ask before sending.
- Passwords written on paper are always unsafe.
- Write only a hint or a reminder, not the full password, if you must note it.
- Banks never ask for passwords by phone.
- If someone asks for your password by phone, hang up and call the bank.
- If an app is official, everything it asks for is safe.
- Check permissions and ask an official worker if unsure.

3. Facilitator answer key (one-line explanation for each card):

Myth — Apps do not magically recover passwords; recovery usually requires verification steps.

Truth — Reusing passwords means one breach can expose many accounts.

Myth — Longer passwords or phrases are generally much harder to guess.

Freedom Under Password

Technology Literacy

Truth — Official help is safer than sharing private credentials with others.

Myth — Even trusted people can be compromised; sharing increases risk.

Truth — Always ask for help without giving your password.

Myth — Not all symbols add meaningful strength; structure and length matter.

Truth — A long, unique phrase (a passphrase) is both memorable and strong.

Myth — Having a phone number alone does not grant access; additional verification is usually needed.

Truth — Ask why an ID photo is needed and who will store it before sending.

Myth — Paper can be safe if stored securely; avoid writing full passwords in obvious places.

Truth — A hint or reminder is safer than the full password on paper.

Myth — Scammers may claim to be banks; banks do not ask for passwords by phone.

Truth — Hang up and call the bank's official number to verify.

Myth — Official apps can still request unnecessary data; check and ask.

Truth — Always check app permissions and ask an official worker if unsure.

3. Summarize the three most common misconceptions you observed.

Freedom Under Password

Technology Literacy

4. Reinforce three simple rules: (1) don’t share passwords; (2) use long unique phrases; (3) ask official helpers when unsure.

Notes

Poster text:

- Big letters: TRUTH (green) and MYTH (red).
- Add a pictogram under each: padlock under TRUTH, warning triangle under MYTH.
- Low-literacy options: Read cards aloud and use pictograms on each card.
- Allow participants to point instead of moving physically.

Co-funded by the European Union. The opinions and views expressed in this document are those of the author(s) alone and do not necessarily reflect those of the Servicio Español para la Internacionalización de la Educación (SEPIE). Neither the European Union nor the issuing authority can be held liable for them.