Protect the Learning Portal

A fictional paper-only activity. Never enter or share real passwords or account details.

THE SCENARIO

A community learning portal lets people sign in, open lessons, and save progress. Some users share a library computer. Your mission is to help protect the people using it.

1 Draw the system

LEARNER — A person → **DEVICE** — Shared or personal → **PORTAL** — Login + lessons → **RECORDS** — Private data

On your drawing: circle TWO things to protect and mark ONE place access should be checked.

One trust check I would add: _____

2 Choose two valuable assets

- ☐ Private learner information
- ☐ Saved progress and assignments
- ☐ Sign-in access
- ☐ Lessons being available

Why do your two choices matter to the people using this system?

_____

_____

REMINDER: You are defending an imaginary service. Do not click suspicious links, test real systems, or include private information on this page.

Find the risk. Choose the safeguard.

Write brief answers; complete the activity without a computer or an account.

3 What could go wrong?

A A message pretends to be staff and demands a password immediately.

Asset at risk: _____

B Someone leaves a shared computer while still signed into the portal.

Asset at risk: _____

C A shared device has not installed available security updates.

Asset at risk: _____

4 Choose a defense for each scenario

Options: report suspicious messages; MFA/passkey; sign out; software updates; recovery support.

A → _____

B → _____

C → _____

5 Suggest one improvement and a safe way to check it

Use this sentence: “I would add ___ because ___. I would check it by ___.”

_____

_____

_____

GO DEEPER: Would your safety improvement make signing in harder for someone using assistive technology or needing account recovery? How would you address that?

Worked example + self-check

Compare explanations, not only answers. There can be more than one reasonable approach.

EXAMPLE ASSETS & BOUNDARIES

Assets: account access, saved work, private information, and lesson availability. Boundaries: check identity at sign-in and authorization before accessing another learner’s records.

SCENARIO	USEFUL SAFEGUARDS
A — fake message	Use a known channel to verify or report it. Do not share codes or passwords. MFA may help, but it is not absolute protection.
B — shared computer	Sign out, provide a visible reminder, and use sensible session timeouts and support.
C — updates	Use trusted automatic updates where possible and define who maintains shared devices.

FOUR QUESTIONS — QUICK SELF-CHECK

1. What is one valuable thing to protect?
2. How is a threat different from a weakness?
3. How can you verify an urgent message safely?
4. Why should we test a protective measure?

TAKEAWAY

A useful threat model names something valuable, a plausible concern, a protective choice, and a way to check whether it helped.

Keep learning: CISA Secure Our World • OWASP Threat Modeling • gunnchos.com