HOW DO HACKERS AND DEFENDERS THINK?

WEEK 7 | DEFENSIVE CYBERSECURITY

Learn to recognize risks, protect people and information, and design safer systems — with nothing more than paper and pencil.

Public & self-guided

No laptop required



What matters?
What could go wrong?
What would help?

Choose the depth that helps you

You can start anywhere. The same scenario supports three levels of learning.

EXPLORER

Recognize an everyday risk. Explain one way to protect yourself or someone else.

BUILDER

Draw a simple system. Choose safeguards, then explain how you would test them.

ENGINEER / RESEARCHER

Identify trust boundaries, compare mitigations, and describe the evidence needed to validate a security decision.

START HERE

Security starts with ordinary moments

A safe learning account, a borrowed laptop, or a surprising text message.

1

A SCHOOL PORTAL

Can someone else get into your work?

2

A SHARED DEVICE

Did you remember to sign out?

3

A URGENT MESSAGE

How can you check whether it is real?

TODAY'S QUESTION

What would you protect first — and how would you know it was protected?

A defender makes a plan before a problem happens

A simple threat-modeling loop based on OWASP.

1 WHAT?
What are we protecting?

→

2 WHAT IF?
What could go wrong?

→

3 WHAT NEXT?
What should we do?

→

4 DID IT WORK?
How would we check?

IMPORTANT Good cybersecurity is a repeatable way to ask and answer questions.

FICTIONAL SCENARIO

Meet the Community Learning Portal

A made-up example — not an actual website or an invitation to test one.



The portal should let authorized people learn safely.

It should also stay available, preserve work correctly, and limit who sees private information.

What has value in this system?

An asset is something worth protecting. People and trust matter too.

ACCOUNT ACCESS

Who is allowed to sign in?

PRIVATE INFORMATION

Names, records, and personal details.

LEARNER WORK

Correct files, progress, and assignments.

SERVICE TIME

People can reach the lessons when needed.

Threat ≠ vulnerability ≠ risk

Three helpful terms; you do not need to memorize them immediately.

THREAT

Something that could cause harm.

A fake account message.

VULNERABILITY

A weakness that harm could use.

A reused password.

RISK

The chance and consequence of harm in context.

Someone gets into a learner account.

Different questions, different responsibilities

Understanding potential harm helps defenders prevent it — the goal here is protection.

POTENTIAL MISUSE

What could be abused?

A message might impersonate staff. A shared device might expose a signed-in account. A bug might interrupt lessons.

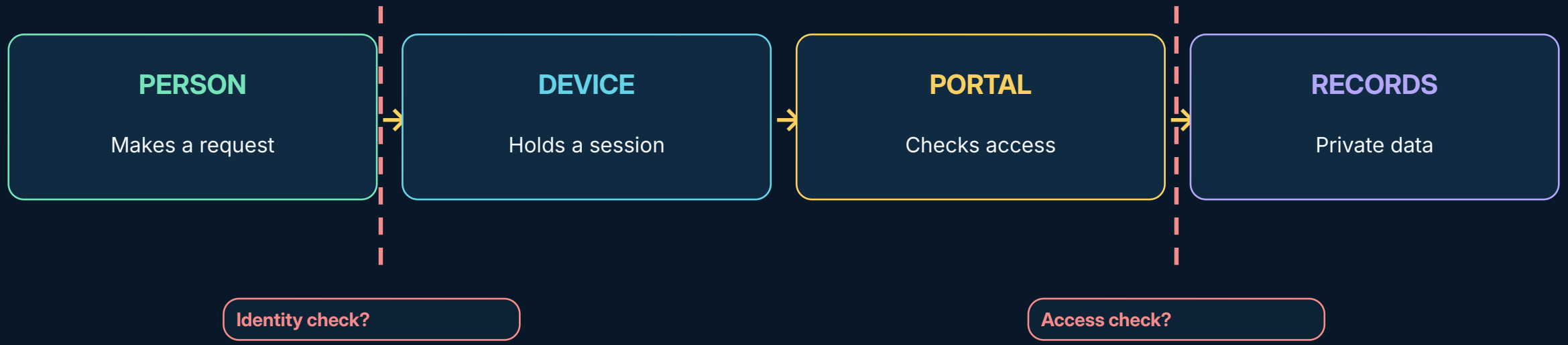
DEFENSIVE MINDSET

How do we protect people?

Verify identity. Limit access. Patch systems. Provide safe recovery paths. Monitor for problems.

Where does trust change?

A trust boundary is where the system must check who or what is allowed.



ASK

At each boundary: Who is requesting access? What should they be allowed to do?

An urgent message is not automatically trustworthy

Fictional example: no real link or account information is needed.

ILLUSTRATIVE MESSAGE - NOT REAL

“YOUR LEARNING ACCOUNT WILL CLOSE TODAY! VERIFY NOW!”

Sent from an unfamiliar address; asks you to enter your password.

QUESTIONS

Who sent it?

Why the urgency?

Can I check another way?

Should I report it?

Stop → Check → Report

If something feels wrong, slowing down is a useful skill.

STOP

Do not rush, click, or share secrets

→

CHECK

Open the official app or known website yourself

→

REPORT

Tell the trusted organization or adult

SAFETY

Never share passwords, one-time codes, private records, or screenshots of them.

Four everyday ways to reduce risk

These four habits reflect CISA's "Secure Our World" guidance.

1 **RECOGNIZE & REPORT**

Phishing or suspicious requests

2 **UNIQUE PASSWORDS**

Long, unique logins; manager helps

3 **USE MFA / PASSKEYS**

Extra protection when available

4 **KEEP SOFTWARE UPDATED**

Security fixes and safer defaults

Passwords, passkeys, and multifactor authentication

Protect the sign-in process without making it impossible for real users.

PASSWORDS

Use unique, long passwords. A reputable password manager can help you generate and store them.

PASSKEYS & MFA

Use passkeys when supported and an additional sign-in factor when offered. Keep recovery options safe.

DO NOT DO

Never type real passwords or one-time codes into a public activity, chat, or worksheet.

Protection also means preparing for mistakes

An update fixes known weaknesses; a backup helps when something is lost or damaged.

UPDATE SOFTWARE

Install trusted security updates for your own device and apps. Use automatic updates when practical.

PLAN FOR RECOVERY

Keep safe backups where appropriate. Know the official place to request account recovery or support.

REAL WORLD

Good safety tools should help people recover without creating more harm or confusion.

Confidentiality • Integrity • Availability

A classic way to organize what needs protection.

C

CONFIDENTIALITY

Private learner records stay private.

I

INTEGRITY

Assignments and scores stay accurate.

A

AVAILABILITY

Lessons are reachable when needed.

Layers of protection work together

No single safeguard solves every problem.

1	VERIFY IDENTITY	MFA, passkeys, safe sign-in
2	LIMIT ACCESS	Only the permissions a person needs
3	MAINTAIN SYSTEMS	Updates and secure configurations
4	NOTICE & RECOVER	Reports, backups, and support

Not every risk deserves the same response

Consider likely harm, who could be affected, and how sure you are.

POSSIBILITY

What conditions might make this problem plausible? What evidence is missing?

CONSEQUENCE

Would it expose private data, change records, or interrupt learning?

PRIORITY

What can we improve first, with the time and resources available?

Your mission: protect the learning portal

A 10-minute paper challenge. You can work alone, in a pair, or with a guardian.

THE FICTIONAL PORTAL

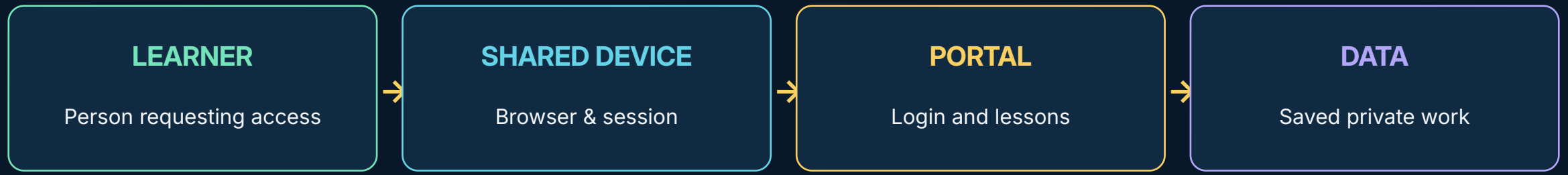
Learners sign in to read lessons and save progress. Some people use shared library computers. Staff can help with accounts, and private information must stay protected.

YOUR GOAL

Identify assets, three risks, and safe protective choices. Explain how you would check whether they help.

Draw the system and its boundaries

Copy this simple map on paper; you may add more boxes if useful.



YOUR TASK **Circle two assets. Draw a dashed line where a trust check is needed.**

HINT Who is allowed to access the records? How would the portal know?

Choose what matters most

Pick TWO assets and explain who is harmed if they are lost or exposed.

A **PRIVATE RECORDS**

Avoid exposing learners' personal information.

B **LEARNING PROGRESS**

Keep saved work accurate.

C **SIGN-IN ACCESS**

Only the right person can enter.

D **SERVICE ACCESS**

People can open lessons when needed.

Find three things that could go wrong

The scenarios are fictional. You are not asked to reproduce them.

A A message claims to be staff and demands an immediate password “verification.”

B A learner leaves a shared computer while still signed in.

C A public device repeatedly postpones important software updates.

Match protections to the concerns

More than one safeguard can be useful for each situation.

1. Report suspicious messages through a known channel
2. Use strong, unique account access and MFA if supported
3. Sign out and protect access on shared devices
4. Keep software and browsers updated
5. Offer safe, accessible account recovery

ACTIVITY 5

Design a security improvement that people can use

Security that locks out a legitimate learner is a problem worth addressing too.

CHOOSE

Pick one concern

→

IMPROVE

Add a safeguard

→

TEST

What safe evidence shows it helped?

TRADEOFF

Could a new safeguard confuse people, block access, or require an accessible alternative?

Write: “I would add ___ because ___. I would check it by ___.”

PAUSE HERE

Your threat model is now an artifact

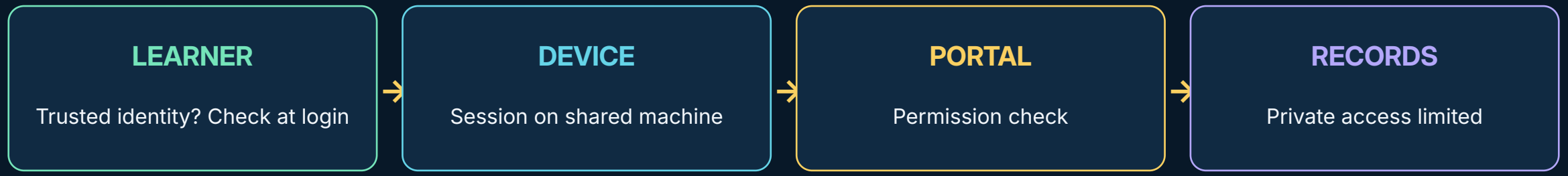
Before checking the worked solution, see whether you completed each step.

- [ ] A system map with at least one trust boundary
- [ ] Two assets and why they matter
- [ ] A concern and protective choice for A, B, and C
- [ ] One improvement with a safe validation idea

REMEMBER There is no single perfect diagram. Compare your reasoning, not just the final boxes.

Example map: assets and trust boundaries

One defensible answer — other reasonable designs are possible.



ASSETS

Account access, private records, learner work, and lesson availability all matter. A trust check belongs at sign-in and before reading someone else's records.

Example protections — and what they do not solve

Matching a defense is about reducing risk, not promising perfection.

A FAKE MESSAGE	Report through a known channel; never share a code. MFA also helps protect sign-in.	Does not eliminate all social-engineering risk.
B SHARED DEVICE	Sign out; use session timeouts and clear user cues.	A logout prompt may be overlooked.
C OUTDATED APP	Maintain updates and a clear device owner.	Updates alone do not solve every issue.

Respond safely. Get help. Recover.

A security mistake is a reason to act, not a reason to hide.

1	**STOP AND CONTAIN**	Pause the suspicious interaction; avoid further sharing.
2	**USE TRUSTED SUPPORT**	Contact the organization through a known method.
3	**RECOVER SAFELY**	Follow legitimate account recovery, updates, and review steps.

Three safe things to check on your own device

No real passwords, codes, or private screens should be shown or shared.

CHECK UPDATES

Find the device’s update section. Do not install random links.

CHECK ACCOUNT SECURITY

Review if MFA or passkeys are available through official settings.

CHECK REPORTING

Find where your school, bank, or service accepts safety reports.

Design a safer sign-in for a community library

Protect people without making ordinary learning harder.

GOAL	Members can sign in reliably
THREAT	An impersonating message asks for secrets
CONTROL	Verified notices + MFA/passkey + reporting
TEST	Try a fictional review scenario with volunteers

Go deeper: six questions for a system review

STRIDE gives engineers categories for asking what might go wrong.

S **SPOOFING**

Who might pretend to be someone else?

T **TAMPERING**

What information could change improperly?

R **REPUDIATION**

How could important actions be disputed?

I **INFO DISCLOSURE**

Who could see something private?

D **DENIAL OF SERVICE**

What could interrupt the lessons?

E **PRIVILEGE INCREASE**

Could someone gain access they should not have?

Four questions before you finish

Try answering them in your own words before advancing.

1. What is an asset in our fictional portal?
2. How is a vulnerability different from a threat?
3. What is one safe response to an urgent “verify now” message?
4. Why is a security control not the same as a guarantee?

One set of clear, defensible answers

Your own wording is fine if your reasoning matches.

1. An asset: learner work, private data, sign-in access, or usable lessons.
2. Threat = potential harm. Vulnerability = weakness that could allow it.
3. Do not click. Independently check through the official service and report.
4. Safeguards reduce risk but may fail, be bypassed, or create tradeoffs.

Leave with an answer, an artifact, or a better question

What protective idea would you carry into the real world?

EXPLORER

Tell someone one safe online habit you learned.

BUILDER

Keep your annotated portal threat model.

ENGINEER / RESEARCHER

Record one unresolved tradeoff and the evidence needed.

SHARE

What would you protect first — and how would you check that your choice helped?

Keep learning — safely and freely

Official references, open learning pathways, and the next Thursday topic.

CISA — SECURE OUR WORLD	cisa.gov/secure-our-world
OWASP — THREAT MODELING	owasp.org/projects/threat-modeling-project
NIST — RISK ASSESSMENTS	csrc.nist.gov/pubs/sp/800/30/r1/final
gunnchOS3k	gunnchos.com
THURSDAY TECH LAB	gunnchos.com/labs/thursday
WAIKE + THE TECHNOLOGY LANDSCAPE	github.com/gunnchOS3k

NEXT WEEK • NOV 19 • HOW DOES AN APP OR VIDEO GAME BECOME REAL?