

Tabletop Experience:

The AI Prompt Challenge

Overview

AI tools help us work faster, but using them the wrong way is dangerous. While an approved tool offers better privacy than a public one, the way you interact with it can still create significant security vulnerabilities. That's why practising prompt safety is essential.

For example, poorly structured prompts can result in misleading conclusions from inaccurate AI output and allow unauthorised access to high-level information. This activity focuses on using an official approved tool to improve your workflow, all while following prompt safety best practices.

Roles

Facilitator:

Controls exercise pace, guides discussions and ensures full participation.

Participants:

Openly discuss their thought processes and respond to scenarios in accordance with the exercise rules.

Introduction

Give the participants this scenario: Your organisation approved an AI tool for all employees. This means you have a private lane where your data is not shared with the public. Still, you must follow the safety policies below for creating prompts:

- Never input Personally Identifiable Information (PII) (e.g. names, IDs, birth dates) or Protected Health Information (PHI)
- Do not use trade secrets and confidential documents to create prompts
- Do not input bank details, login and passwords to the AI tool

By the end of the first month, your manager shared a prompt usage report and asked your team to discuss the prompts and sort them into safe and unsafe categories.

Part 1: Signs Annotation

 **Duration:** 15 minutes

Materials:

- Timer or stopwatch
- Scenario handouts
- Pens or pencils
- Paper sheets or notebooks

Instructions:

- Divide the room into small groups.
- Hand out the scenario prints and pens or pencils to each group.
- Read the list of prompts on the handout.
- Instruct groups to underline elements that describe safe AI practices. Examples include using broad statements and not adding specific project and client names.
- Direct groups to **circle** behavioural warning signs. Examples include feeding sensitive data and confidential information to AI systems.
- Explain the importance of following the organisation's policies to make sure you always use authorised content.
- Discuss as a group: How could you rewrite the unsafe prompts to make them safe? Which safe prompts would be useful for your daily tasks?
- Give the groups 15 minutes to discuss the scenario and take notes.

Part 2: Discussion

 **Duration:** 10 minutes

Questions:

- What warning signs did you spot?
- What warning signs initially tricked you?
- Which safe practices for utilising AI were you familiar with?
- How do you practise prompt safety during your daily work and in your personal life?

Possible answers/prompts:

- Prompts used to help employees with routine tasks don't involve confidential information. The employees are using an approved internal tool, so these prompts are safe. The data is not used to train public models.
- Warning signs: Risking personal security, mixing private personal data with work tools and disclosing proprietary information.

Conclusion

 **Duration:** 5 minutes

Wrap up the exercise by connecting the concepts directly to your organisation's reality. Explain that spotting a warning sign is only the first part of the defence; the second is taking the correct action by following the organisation's policies.

Take the opportunity to answer any questions participants may have about creating safe prompts in the workplace to improve AI use.

Exchange experiences and thoughts on AI use in the workplace and share best practices.

Attachment – Facilitator answer key

ID	The Employee's AI Prompt	Category
A	Generate 10 catchy headlines for our new logistics tracking service.	Safe: Using AI for creative brainstorming.
B	This is my to-do list for the week. Organise the tasks by complexity for the best use of my time.	Safe: Using the tool for organisation within the secure 'private lane' to optimise your work.
C	Write a summary of this confidential merger document for the CEO.	Unsafe: Even in secure tools, highly sensitive documents often follow extra rules about where they can be uploaded. According to the scenario safety policies, this action is a violation.
D	Draft a reply to a customer who is happy with our new Berlin warehouse.	Safe: Describing general information to improve communication.
E	I'm logged in as a guest. Here is my personal bank password. Can you help me remember it?	Unsafe: Never enter passwords into any AI tool, even approved ones.
F	Draft a polite email to a colleague asking for an update on a task that was due yesterday, ensuring the tone remains collaborative.	Safe: Requesting text improvements for routine workplace tasks.
G	This is a list of our top customers' full names, birthdays, locations and the date they started working with us. Draft creative personalised birthday messages for them.	Unsafe: Entering Personal Identifiable Information (PII) to AI tools is an unsafe practice. Do not specify customer personal information in your prompts.
H	Explain the core differences between a 'Project Manager' and a 'Product Manager' role in a tech startup environment.	Safe: Asking a high-level question without disclosing proprietary details.

Attachment – Scenario handout

Analyse the following prompts and sort them into ‘safe’ and ‘unsafe’ categories according to the scenario safety policies:

ID	The Employee’s AI Prompt	Category
A	Generate 10 catchy headlines for our new logistics tracking service.	
B	This is my to-do list for the week. Organise the tasks by complexity for the best use of my time.	
C	Write a summary of this confidential merger document for the CEO.	
D	Draft a reply to a customer who is happy with our new Berlin warehouse.	
E	I’m logged in as a guest. Here is my personal bank password. Can you help me remember it?	
F	Draft a polite email to a colleague asking for an update on a task that was due yesterday, ensuring the tone remains collaborative.	
G	This is a list of our top customers’ full names, birthdays, locations and the date they started working with us. Draft creative personalised birthday messages for them.	
H	Explain the core differences between a ‘Project Manager’ and a ‘Product Manager’ role in a tech startup environment.	