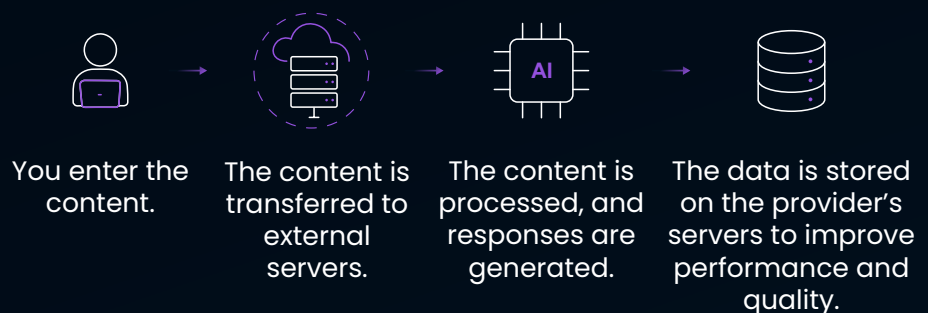


Data Leakage Through AI

AI tools have become an essential part of the workplace, helping to speed up tasks and organize ideas. However, entering internal information or files not intended for sharing into public AI tools may lead to data leakage and privacy violations.

How Do AI Tools Work with Data?



Therefore, data is not always limited to temporary use; it may be processed outside the organization's control.

Risks of Using Public AI Tools in the Workplace



Leakage of work-related data through uploading internal work files



Sharing documents not intended for public release



Privacy violations



Violation of information security and privacy policies



Exposure of details about internal systems or procedures

The Verification Rule and Highly Sensitive Data

Before using any AI tool at work, apply the **"Verification Rule"** by asking yourself:

- ✓ Is this information intended for internal use only?
- ✓ Has the tool been officially approved by the workplace?
- ✓ Can this content be shared without putting the organization's privacy at risk?

Make sure it does not contain any of the following highly sensitive data:

- ✗ Customer or employee data
- ✗ Internal source code
- ✗ Financial and operational data
- ✗ Passwords and access keys
- ✗ Unannounced plans and strategies

This rule aims to prevent any sensitive information from being shared unintentionally with external tools, even in simple use cases such as summarization or improving wording.



Cyber Knowledge:

Do you know what **Shadow AI** is?

It refers to the use of AI tools within the workplace without official approval from the organization or supervision from the IT department. This includes using personal accounts or unauthorized external services to complete work-related tasks. Its risk lies in creating an invisible flow of data outside the scope of security governance, which may lead to sensitive information being leaked or stored in systems that are not subject to the organization's policies or oversight.



Real-Life Incident:

In 2023, Samsung Electronics recorded internal incidents related to the use of public AI tools such as ChatGPT in the workplace. Some engineers entered internal source code and content from work meetings to improve code or summarize text. However, this data was sent to external platforms for processing, raising security concerns about sensitive information leaving the organization's environment.



Lesson Learned:

The company-imposed restrictions on the use of public AI tools within the workplace.



You can view the details of the incident by scanning the code

Cybersecurity Measures When Using AI Tools at Work:



Use AI only for general tasks, such as drafting, summarizing, and non-sensitive translation.



Do not enter any internal data or information that can be directly linked to or identify the organization.



Replace sensitive data with general or placeholder information when needed.



Use only tools approved by the workplace.



Review the privacy policy before using any external tool.



Report any unintentional sharing of sensitive data to the IT team.



AI is an effective tool for increasing productivity at work. However, using it without proper awareness may put sensitive work data at risk of leakage.

Use AI wisely, and do not enter the organization's data outside the secure work environment.

