

International Conference

Strengthening Cybersecurity Awareness and
Best Practices

**Tools Developed and Adapted under MECyS:
Chatbot Demonstration and Selection of
Further Tools.**

Jens Alber, University of Education Freiburg (Coordinator of MECyS)

PH Freiburg – 10 Apr 2025

MECYS – TOOLS

Objectives

Creation of tools

Presentation of selected tools

Chatbot demonstration



MECYS TOOLS – OBJECTIVES

- creation of a set training tools and materials, partially adapted from identified best practices
 - adaptation of learning tools generated in GEIGER
 - creation of further learning tools
- testing of tools in pilot workshops
- implementation of tools into National Course Plans
- translation of tools
- making tools freely available:
 - Moodle platform
 - (OER) repositories
 - Kahoots

CREATION OF TOOLS

- tools discussed during workshop in Paris, June 2023
→ Report Learning Tools
- country- and target group-specific creation and refinement of tools
- discussion of implementation of tools during workshop in Larisa, Oct 2024
- some tools used by several or even all partners (e.g. Chatbot)

SECURE SME (ENISA)

- <https://tools.enisa.europa.eu/securesme#/>
- How to secure your employees and business from cyberattacks?



Cybersecurity doesn't necessarily have to be costly for SMEs to implement and maintain. There are several measures that can be implemented, without the company having to invest a large amount.

Cyber Tips



Discover all Cyber Tips



Protect Employees



Enhance processes



Strengthen technical measures



Overcome COVID19 issues

CYBERSECURITY MATURITY ASSESSMENT FOR SMES

- <https://tools.enisa.europa.eu/cybersecurity-maturity-assessment-for-small-and-medium-enterprises#/>

The screenshot displays the user interface for the 'Cybersecurity Maturity Assessment for Small and Medium Enterprises' tool. The page features a dark blue header with the title, a grey sidebar on the left with a call-to-action button, and a main content area with three sections: '3 reasons to assess your company's cybersecurity maturity', '3 key areas to assess for your business', and a 'Start the assessment' button.

Cybersecurity Maturity Assessment for Small and Medium Enterprises

This tool helps Small and Medium-sized business enhance their cybersecurity maturity level and provide them with an adaptive progressive plan to handle cybersecurity risks.

[Start the assessment >>](#)

3 reasons to assess your company's cybersecurity maturity

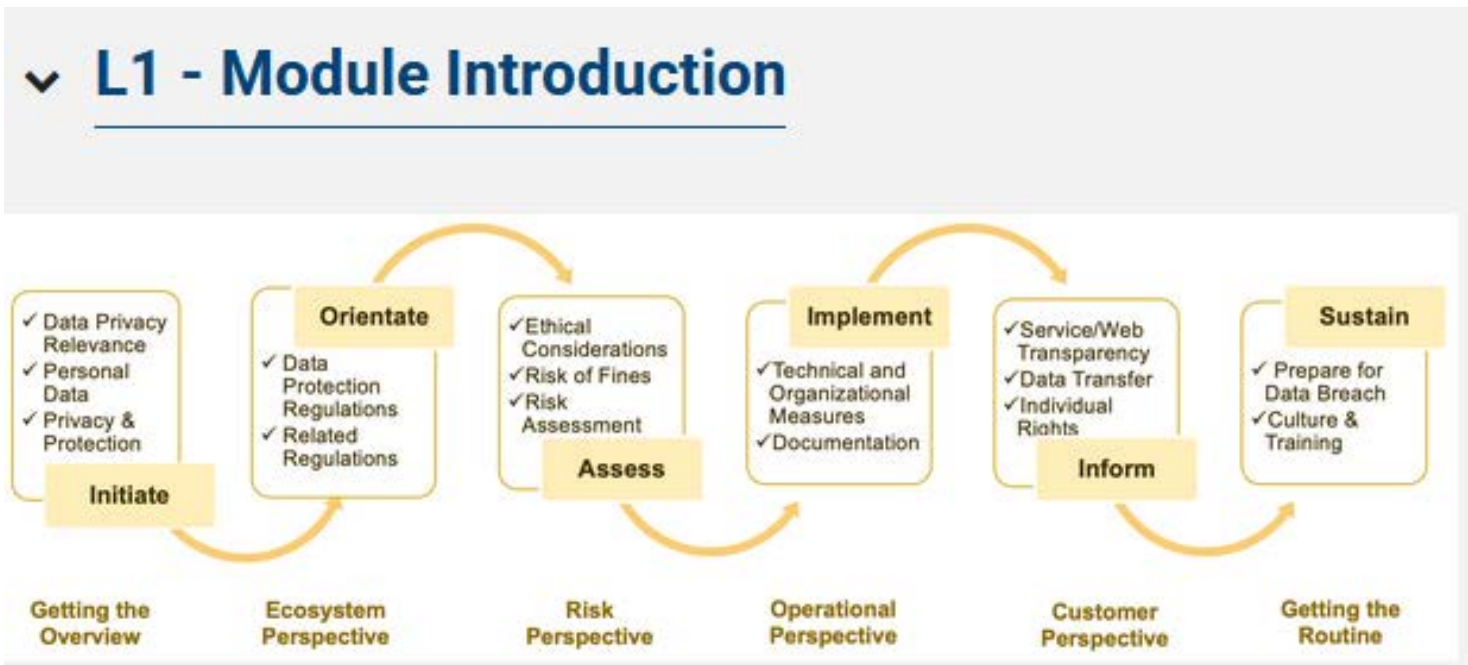
- Cybersecurity evaluation**
Understand what is your cybersecurity maturity level and compare with similar businesses
- Personalised plan**
Get a tailored improvement action plan adapted to the needs of your business
- Top security**
Use our online secure tool to increase your cybersecurity level with our recommended action plan

3 key areas to assess for your business

- People**
Assess whether your employees are prepared to face cyber threats
- Technology**
Understand your technology and how to implement best cybersecurity practices
- Processes**
Ensure that your organisation has the right processes in place to deal with cybersecurity risks

DATA PRIVACY FUNDAMENTALS COURSE PACKAGE

- 10 lessons on data privacy and data protection compliance



KAHOOTS



Classic mode

Up to 200 players Competition Assessment

Bring friendly competition to this kahoot. Players go head-to-head and compete for a top spot on the podium. Players who answer the quickest and get the most correct answers will have higher scores.

Content

Your parcel could not be delivered. Confirm your delivery details here: www.nakej-vertobajuni.link*

Lerntool Mysec_english

Start

- Learningtool Mysec
- Cybersecurity
- Phishing

COURSE UNIT ON PHISHING FOR (VOCATIONAL) STUDENTS

- two lessons at school
- instructions on order and content of tasks
- contains self-study modules, elements to be discussed in class, tasks with Cybersecurity Chatbot as well as Kahoot Quiz

Instruction on self-study course

Recognizing and understanding phishing

Target group: (Vocational) students

Topic: Phishing – Recognising, Understanding, Avoiding (protection strategies)

Duration: 2 Modules with in-depth self-study task using the Cybersecurity Chatbot in between

Module 1: Introduction to “Phishing”

Step 1: Read introductory text

Step 2: Answer questions on “Phishing” (ca. 20–30 Minutes)

Step 3: Homework with the chatbot

Module 2: In-depth study and application of phishing

Step 4: Introduction and revision

Step 5: Edit worksheets

Worksheet 1: Analyzing phishing emails

Worksheet 2: Develop one's own protection strategies

Step 6: Reflection and conclusion

Course objectives

At the end of the course you will be able to:

- Detect phishing attacks with confidence.
- Identify typical features of phishing emails.
- Develop concrete strategies to protect yourself and others.

MECYS CHATBOT – DEMONSTRATION

- <https://cybersecurityassistant.rhieszeros.ch/mecys/>



The screenshot shows the MeCys Assistant interface. At the top left, there is a logo with a checkmark and the text "MeCys Assistant". Below the logo, there are two main options for starting a conversation:

- A blue button labeled "Create New Conversation".
- A section for loading an existing conversation, which includes a text input field labeled "Enter conversation ID" and a blue button labeled "Load Conversation".

- available in several languages
- Feel free to broaden your knowledge using it 😊

THANK YOU!

mecys.eu



Co-funded by
the European Union