MECyS | Micro Entreprise Cybersecurity

International Conference

Strengthening Cybersecurity Awareness and Best Practices

The MECyS Project: Objectives and Target Groups

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

PH Freiburg – 1o Apr 2025

Pädagogische Hochschule Freiburg
Université des Sciences de l'Education · University of Education

Co-funded by the European Union

CONTEXT OF MECYS – MICRO-ENTREPRISE CYBERSECURITY

HTTPS://MECYS.EU/

Background and objectives

- Partners
- Objectives, target groups and key stakeholders

Previous results

- Reports, Workshops, Course Plans

Dissemination

- National and International Conferences and Events, Social Medica, etc.

MECYS BACKGROUND AND OBJECTIVES

- MECyS is kind of a follow-up project of ‚GEIGER‘ (https://project.cyber-geiger.eu/)
  - “Easy and affordable cybersecurity solution for small businesses”
- (New) partner with different backgrounds
  - Anemo (Paris), Fachhochschule Nordwestschweiz (Basel), A.B. INSTITUTE OF ENTREPRENEURSHIP DEVELOPMENT (Polis Chrysochous, CY), Association of Thessalian Enterprises and Industries (Larissa, GR), CENTRO SUPERIOR DE FORMACION EUROPA SUR (Malaga)
- Development of cybersecurity skills and competences among **non-IT staff** to enhance digital resilience
  - Development and adaptation of courses and teaching/learning materials for cyber security and data protection for IT laypersons in small companies and organizations (SMEs).

TARGET GROUPS / KEY STAKEHOLDERS

- Non-IT staff in Micro and Small Enterprises (MSEs)
- Employees, managers/owners, volunteers
- Individuals undergoing formal vocational training
- Family members

RESULTS SO FAR

- Project duration: 1/23 to 4/25 (final phase)
- Project schedule
  - Theoretical basis in 2023 – Piloting phase – Implementation – **Dissemination**
- Theoretical basis
  - Report on Learning Hurdles (qualitative and quantitative survey)
  - Overview on Vocational Education in Cybersecurity and Data Protection
    - 'Comparison' of the location in the vocationally oriented education systems of the partner countries
  - Overview (Interactive) Learning Resources / Report Learning Tools
  - Prototypes – Learning Plans
    - Based on common workshop in Paris

REPORT LEARNING HURDLES
OVERALL SUMMARY AND CONCLUSIONS

- While MSEs exhibit a clear understanding of the risks, their actions often diverge from this awareness. Potentially, this might be due to limited resources hindering the clear separation of private and work devices.
- Passwords are considered safe; nevertheless, 2-Factor Authentication is used, possibly due to technological requirements.
- There are contradictions concerning trust in bigger companies: They are trusted in concern of cybersecurity but not in concern for data protection. However, in reality, this issue is more complex and not easy to distinguish.
- Participants agree to being tracked online for purposes that only serve the company (and not necessarily themselves), but they also expect their data to be protected from big companies. These results might possibly indicate an acquiescence bias.
- There is a perceived positive impact of data protection. Negative impacts concern especially insecurities and added bureaucratic measures. The consent form is perceived as negative by participants.
- Overall, there are ambiguities between risk aware knowledge, rather pragmatic behaviour and divergent attitudes to data protection.

NATIONAL COURSE PLANS

- Detailed learning paths for each target group in the respective partner country, including settings and tools
- Development/adaptation of tools
- Course Plans adapted after Testing in Pilot workshops and implementation in National Training Prototypes
- Objective: available in English + national language at the end of the project

DISSEMINATION

- Presentation of project results:
  - Project website: https://mecys.eu/
  - Moodle platform: https://campus.mecys.eu/
  - National conferences and events
  - International Stakeholder Conferences
    - 12 March: Understanding Your Role in Cybersecurity
    - 10 April, 14:00-17:00 CET: Strengthening Cybersecurity Awareness and Best Practices
  - (OER) Repositories
  - etc.
- Further activities to raise awareness for cyberthreats and inform about events:
  - Social media channels
    - LinkedIn
    - Facebook
    - Instagram

MECyS | Micro Entreprise Cybersecurity

THANK YOU!

mecys.eu

Co-funded by
the European Union