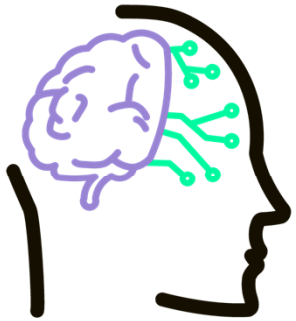


ITCYBER

INTERMEDIATE TOPICS IN CYBERSECURITY

Intermediate Topics in Cybersecurity

Konstantinos Karampidis[1], Emmanouil Lionakis[1], Giorgos Papadourakis[1], Giorgos Kornaros [1,] Przemyslaw Szczepanczyk[2], Rui Silva[3]

[1]Hellenic Mediterranean University Heraklion, Greece , [2]Lipinski University, Kielce Poland , [3]Instituto Politécnico de Beja, Beja Portugal

Co-funded by the Erasmus+ Programme of the European Union

About

- **Cyber II** (Intermediate Topics in Cybersecurity) is a 3-year project co-funded by the Erasmus+ programme of the European Union, started in September 2024 and it involves 3 partners across Europe.
- Today's challenging digital landscape needs trained people capable to identify potential cybersecurity threats and able to respond adequately when an attack is identified.
- Personnel training in these skills is **costly**.

About

The Cyber II project aims to increase the cybersecurity knowledge by:

- Familiarising them with a set of real-life cyberattack scenarios
- Training them on Cybersecurity through a self-paced learning course
- Improving their knowledge independent of where they are.

Project Partners

- **Coordinator:** Lipinski University, Kielce Poland
- **Partner**: Hellenic Mediterranean University, Crete, Greece
- **Partner:** Instituto Politécnico de Beja, Beja Portugal

Overall Impact

On Higher Vet Centers/ HE Institutions/

- Higher VET/ HE Institutions are invited to integrate a Course for training students in operational cyber security that is practical, adaptable and which meets demands.
- Constant modernization of their organizations and educational offer.

Outcomes – The course

The partnership will develop an advanced course on cybersecurity tailored for todays needs. It comprises of four (4) modules:

Module 1 - Organised disinformation and threats in social media

Module 2 - Standards and recommendations in cybersecurity management

Module 3 - ENISA cybersecurity skills framework

Module 4 - Use of AI in cybersecurity

Outcomes – The course

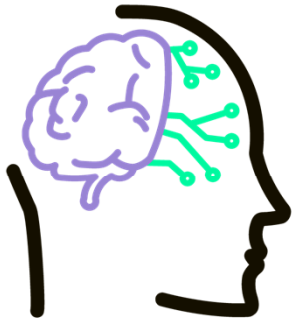
- Module 1 will focus on threats brought about by the malicious use of organised disinformation and is intended to improve the learners' media literacy and resilience to propaganda, fraud, brainwashing, election-rigging and other threats. The module will show common denominators in disinformation attempts (psychological, technical, methodological etc.), present case studies from each country and from Europe and the world in general.
- Module 2 will present the ISO-27000 norms and other best practices and recommendation for cybersecurity, providing the learner with the necessary skills to implement a proper cybersecurity standard at their workplace.

Outcomes – The course

- Module 3 will present the European Cybersecurity Skills Framework and the 12 professional profiles recognised by The European Union Agency for Cybersecurity (ENISA). After finishing this module, the students should have an idea about which career path in cybersecurity they wish to take.
- Module 4 will be an overview of the role AI plays and will play in the future of cybersecurity, cybercrime and disinformation. This aspect evolves very rapidly, and we feel that the students need to learn about the opportunities and threats this poses ASAP.

Next steps

- Announce the Moodle course
- Translate the course in Polish, Greek , Portoguese
- Pilot testing



ITCyber

INTERMEDIATE TOPICS IN CYBERSECURITY

Thank you!

Co-funded by the
Erasmus+ Programme
of the European Union